National Test Bed Security and Communications Architecture Working Group Report

April 1992

NTB NETWORK

SECURITY AND COMMUNICATIONS ARCHITECTURE

July 29, 1991

Accession Number: 4539

Publication Date: Jul 29, 1991

Title: National Test Bed Security and Communications Architecture Working Group

Corporate Author Or Publisher: SDIO, The Pentagon, Washington, DC 20301

Descriptors, Keywords: National Test Bed Security NTBN Communications Architecture Working Group Tiger Team NTB Network

Pages: 00200

Cataloged Date: Jun 23, 1993

Document Type: HC

Number of Copies In Library: 000001

Record ID: 27088

EXECUTIVE SUMMARY

A. INTRODUCTION

The National Test Bed (NTB) Security and Communications Architecture Working Group (SCAWG - also called the "Tiger Team") has developed this report to provide definition of a system architecture, operational concept, and system implementation approach for a secure and integrated information transfer system to support the NTB mission. This new system will evolve from the existing National Test Bed Network (NTBN).

The Tiger Team began its work in March 1991 and met regularly for five months. Initial Tiger Team efforts focused on identifying system requirements and investigating available technologies in the areas of security, automated information systems (AIS) interfaces, communications, and control. The Tiger Team evaluated alternative architectures, operational concepts, and implementation approaches based on their projected cost and responsiveness to system requirements. The Tiger Team's recommendations were approved by representatives of the Government organizations and support contractors identified in Table EX-1.

Table EX-1. Tiger Team Representation

Government Member	Support Contractor
SDIO/POI	BDM International, Inc. (BDM)
SDIO/SIS*	Beta Analytics, Inc. (BAI)
SDIO/SDA*	General Electric (GE)
SDIO/SDT (NTBJPO)	MITRE Martin Marietta
USASDC	COLSA, INC.
NSA	SPARTA

* Government representative not available

B. THE CHALLENGE AND COMPELLING NEED

The need for security in the NTB environment is dictated by the sensitivity of information and the internal and external threat of compromise of that information. Security as such is an enabling technology which provides a wide range of users access to shared computer and communication resources which process information at multiple levels of classification. The challenge in providing the needed security is defined by the environment within which the NTB mission must be performed. The key elements of the mission environment include:

(1) Dispersed geography with many AIS platforms and many requirements to communicate;

(2) A wide range of users from Government, industry, and various U.S. Allies; and

(3) A wide range of security classification levels required.

In order to accomplish the mission within this operational environment, certain fundamental components of infrastructure must be implemented in an integrated manner. These include communications and control, security, and AIS interfaces. These components provide the enabling technologies needed to support secure information exchange among the broad and dispersed NTB user community. The interaction among these components of infrastructure demands that an integrated approach be utilized in defining the system requirements and architecture.

C. REQUIREMENTS

The derivation of security and communications requirements was approached from a mission perspective as well as user (i.e. SDIO organizations and associated contractors that need secure communications services (NTBN) to perform experiments and testing) and operator (i.e. the builders and maintainers of the NTBN) perspectives. Examination of the mission drove the derivation of fundamental requirements for security and communications infrastructure, while the compilation of user and operator views of requirements either validated or refined the fundamental mission-driven requirements.

The NTBN infrastructure must exhibit certain system security and communications characteristics in order to be responsive within the research and development environment. The critical characteristics are flexibility (including growth capability), modularity, and standardization. The requirement for flexibility is derived from both the changing mission environment and the evolution of test phases as cited by the SDIO user community. The requirement for modularity follows the derivation of the requirement for flexibility, and the need to support a shared resource user community. The need for standardization (and conformance to a guiding set of standards) derives from the dynamic nature of the NTBN user community and from public law and DoD policy. *Standardization of security access mechanisms, communications mechanisms, and operational procedures will be essential to maintaining a responsive NTBN over its life cycle.*

Access to data on the NTBN must be restricted to only those users who are appropriately authorized for that data. Authorizations should be based on a user's security clearance, need to know, and restrictions resulting from organizational conflicts of interest.

The user communications requirements presented in Annex 1 to this report were examined in aggregate for trends which may influence the system architecture. Validation of these data through interviews with SDIO personnel could result in minor changes. However, the data are not expected to change enough to affect the general conclusions drawn from the data. The most obvious conclusion which can be drawn from examination of the requirements data is that there is a large and diverse community requiring access to NTB resources. Further, this diverse community requires NTB assets for performing many different types of functions with varying levels of security requirements and data rates. One also notes that requirements change (sometimes significantly) over time. All of these factors validate the secure communications requirements of flexibility, modularity, and standardization.

The consolidated communications requirements data show a large concentration of user requirements originating from the Strategic Defense Deputate (SD). The user survey also indicated a requirement for over 40 T1 communications links. As these data are validated, and as Theater Missile Defense (TD) user requirements are defined, however, both the size and origin of NTBN

user requirements could change significantly. Thus it is essential that the NTBN have a modular architecture to allow for modular growth.

D. RECOMMENDED NTBN ARCHITECTURE

1. Introduction

In defining a responsive NTBN communications and security architecture, a comprehensive examination of feasible architectural alternatives was conducted. The architectural alternatives were driven by the compiled functional requirements. The global set of alternatives may be categorized within two areas: (1) multiple, single level networks, or (2) a single, multilevel secure network. Given that the NTB has requirements to provide processing and data storage for users who do not all have the same access requirements, the NTBN must provide assured separation of user data on the network. This can be provided for by either of the two types of architectures. The overall tradeoff of the two architectures is driven by responsiveness and cost.

The NTB's current configuration consists of several independent networks. Some networks are unclassified; the others operate either in a Dedicated or System High mode with users cleared to the highest level of data processed on the network. The requirements analysis documented in Annex 1 of this report supports the need for several additional single-level networks in order to serve the needs of the NTB's users.

As an alternative to the proliferation of multiple, single level networks, a single, multilevel secure (MLS) network could be employed to support the NTB users. The MLS network architecture could use a single network backbone to provide services to users with different clearances, need to know, and corporate affiliations.

2. Architecture Selection

Following a thorough review of the technology options available for meeting NTBN communications and security requirements, the Tiger Team concluded that establishment of MLS networks is now a realistic alternative to the continued proliferation of the single-level networks. The decision to recommend an MLS NTBN architecture was driven by several key factors. First, it will be prohibitively expensive over the long term to duplicate communications and processing systems for NTB users who have different data access privileges based on their clearance level, need-to-know, and/or corporate affiliation. Second, single-level networks cannot efficiently support the future operational needs of the diverse SDI user community. Finally, the components of a first-generation MLS network are now commercially available as a result of recent industry and Government-sponsored product development and evaluation efforts.

Chapter VI and Appendix A of this report summarize the Tiger Team's evaluation of the following alternative architectures for a secure NTBN:

(1) Architecture 1. This approach uses secure routers to connect MLS LANs to a communications network secured by link encryption devices. The MLS LANs use commercially available network interface units and control processors to meet NTBN communications and security requirements.

(2) Architecture 2. This approach employs the Government-developed BLACKER Front End (BFE) or CANEWARE Front End (CFE) devices as the interface between single-level LANs (or hosts) and a packet switched network. BFE and CFE systems provide Type 1 encryption as well as computer security features.

(3) Architecture 3. This approach combines the security and communications features of Architecture 1 and Architecture 2. BFE/CFE devices provide a packet switched network interface for MLS LANs as well as single-level LANs, and routers provide point-to-point interfaces between MLS LANs.

(4) Architecture 4. This approach uses multiple single-level networks to enforce data security.

The Tiger Team compared the candidate architectures on the basis of compliance with networking standards, security features, communications performance, operational responsiveness, and cost. The Tiger Team ruled out architectures based on proprietary products or protocols in favor of a multi-vendor network environment based on DoD implementation of open system standards. With this approach, the NTBN will benefit from the wide range of new security and communications technologies which will emerge as both industry and Government continue their migration toward open system standards.

The Tiger Team concluded that Architecture 4 is least responsive to test operations within an R & D environment because reliance on multiple, independent networks can prevent efficient information transfer among AISs connected to different networks. In addition, the overall cost of this approach rapidly increases as data security classification levels and other access restrictions are expanded. The limitation of Architecture 2 and Architecture 3 is the slow communications throughput of the BFE devices. When Caneware network interfaces are available, acceptable throughput will be achievable from these architectures.

The Tiger Team selected Architecture 1 as its near-term architecture recommendation because it provides high communications throughput and can be implemented now using commercial products which use open systems protocols.

3. Architecture Implementation Phasing

Although Architecture 1 is the recommended approach, implementation flexibility is maintained by sequencing a prototype acquisition phase that begins at the LAN level and progresses up through the router/gateway level to the backbone network level. In this manner, the option would be retained to migrate to Architecture 3 at the router/gateway level should future commercial and Government developments merit this approach.

E. SYSTEM IMPLEMENTATION PHASING OVERVIEW

The proposed three-part phasing of the MLS implementation is shown in Figure EX-1. The near-term (FY 91-93) and mid-term (FY93-95) phases provide for NTBN upgrading to an initial MLS capability. The long-term (FY95-99) phase involves incorporation of features for increasing MLS security assurance.

In comparing NTBN security goals and requirements to predicted technological advances, great care was taken to be realistic and objective. It is anticipated that the National Security Agency (NSA) will continue to place high priority on evaluating an even greater number of Computer Security (COMPUSEC) products at even higher levels of COMPUSEC trust in the years ahead. Increased assurance of secure operation is gained as products evaluated at higher levels of COMPUSEC trust are incorporated. The increased assurance is indicated by upgrading from a B3 level of trust to an A1 level. (B3 and A1 are the technical terms used by the NSA and DoD to indicate the degree of trust (i.e. assurance of secure operation) that a computer system has achieved.) A system accredited at the A1 level incorporates security products and safeguards that offer significantly higher levels of trust than those needed for B3 accreditation. The NTBN must have the highest possible degree of trust to minimize the risk of security compromise. Therefore, a phased approach is recommended to achieve higher levels of assurance as the technology becomes available.

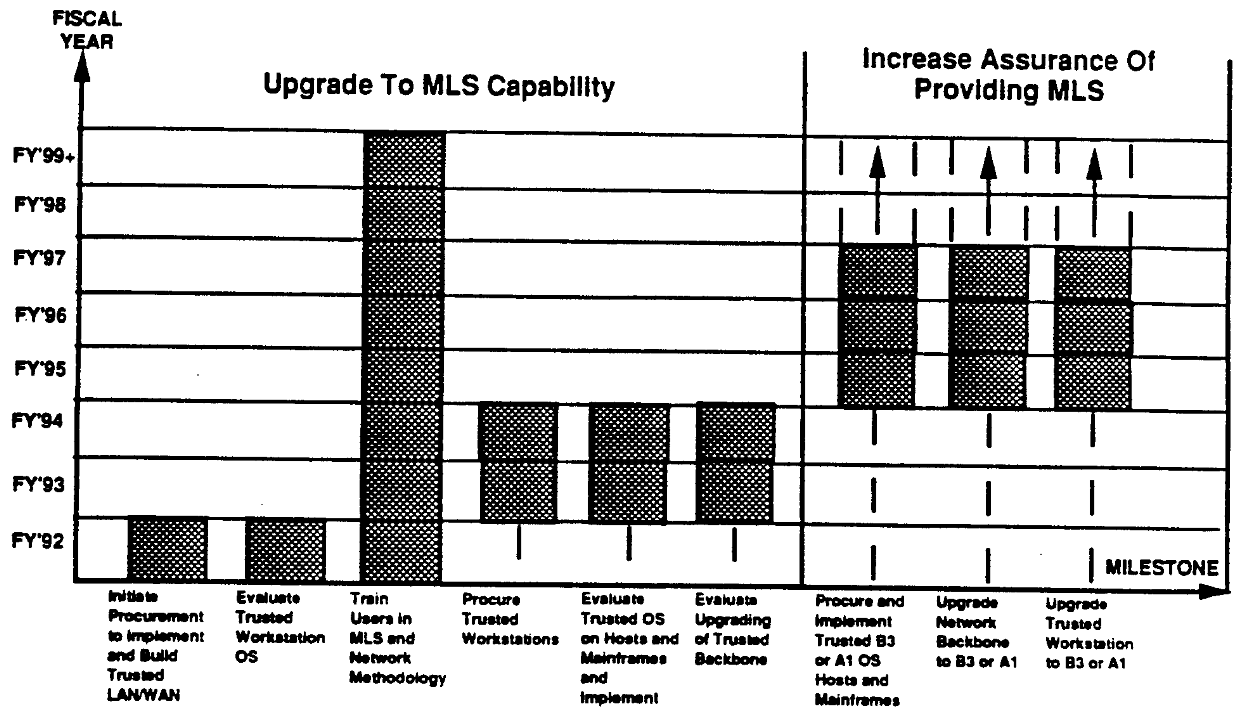


Figure EX-1. Implementation Program Overview

F. CONCLUSIONS

This report recommends a multilevel secure architecture to meet the SDI community's need for a data transfer network which can restrict user access to data based on a range of security considerations including clearance level, need-to-know, citizenship status, and corporate affiliation. The recommendation was driven by three key factors. First, a cost analysis showed that it will be prohibitively expensive over the long term to duplicate communications and processing systems for each set of NTBN users who are not allowed access to the existing set of single-level networks. Second, the proliferation of single-level networks will adversely affect operation by forcing some users to rely on two or more networks to perform a task which could more efficiently be performed on a single, integrated network. Finally, a technology survey showed that components of a first-generation MLS network are now commercially available as a result of recent industry and Government-sponsored product development and evaluation efforts.

The recommended NTBN architecture meets user requirements identified in this report and provides a basis for modular and flexible growth to accommodate new requirements and technologies as they are identified. The selected architecture includes:

(1) A LAN component which conforms to the DoD standard protocol suite and supports secure, high-speed communications with single or multilevel hosts.

(2) An Internet component consisting of secure routers/gateways, which support the DoD protocol suite and secure, high-speed communications with single or multilevel hosts.

(3) A WAN backbone which supports the DoD protocol suite and secure interconnection of NTBN nodes through the LAN and Internet components.

The Tiger Team's recommendations for implementing the recommended architecture include:

(1) Completing the systems engineering, design and planning activities required to gain management approval for procuring MLS networking components.

(2) Installing a first-generation MLS network in FY-92 and performing proof-of-concept testing of key elements of the recommended architecture and detailed network design.

(3) Establishing DAA MOAs to encompass responsibilities and security policies for protection of classified information on AISs and the NTBN.

(4) Establishing an NTBN configuration control board.

(5) Beginning a follow-on effort to define an approach for providing trusted workstations and hosts.

NTBN
SECURITY AND COMMUNICATIONS
ARCHITECTURE

I. INTRODUCTION

The National Test Bed (NTB) Security and Communications Architecture Working Group (SCAWG - also called the "Tiger Team") has developed this report to provide definition of a system architecture, operational concept, and system implementation approach for a secure and integrated information transfer system to support the NTB mission. This new system will evolve from the existing National Test Bed Network (NTBN).

The report consists of eight sections: Section I, Introduction, defines the scope and objectives of the Tiger Team effort reported herein, as well as providing background on the evolution of the NTBN security and communications architecture development. Section II provides a set of basic working definitions used throughout this report. Section III provides an explanation of the challenge and compelling need for an integrated security and communications architecture. Section IV presents the consolidated NTBN requirements derived from an analysis of the NTB mission and interviews with SDIO personnel. Section V describes the basic concepts and technologies available to support an integrated security and communications architecture. Section VI provides a system description of the recommended security and communications approach and is comprised of an operational concept and companion NTBN security and communications system architecture. Section VII describes system implementation tasks including recommended phasing of the required work. Section VIII presents the Tiger Team's conclusions and summary recommendations. Appendix A - Architecture Evaluation provides detailed information which supports the system description presented in Section VI, Appendix B - Guidance and Requirements Document provides preliminary architectures and requirements for evolution to the MLS NTB Communication and Computing System, and Appendix C provides a glossary of terms used in this report. Two annexes are available from SDIO/POI upon request: Annex 1 provides a compilation of user requirements, and Annex 2 provides a compilation of current and future products which will support implementation of the recommended architecture.

A. Scope and Objectives

This document provides a description of an NTBN security and communications architecture, operational concept, and system implementation approach which is intended to assist in planning and implementation of a responsive and secure NTB information transfer system. In addition, representative costing information is provided to assist in financial planning.

B. Background

The Tiger Team is an interim working group formed to define an integrated, secure information transfer system to support the NTB. The team comprises the government members and support contractors identified in Table I-1.

Table I-1. Tiger Team Representation

Government Member	Support Contractor
SDIO/POI	BDM International, Inc. (BDM)
SDIO/SIS*	Beta Analytics, Inc. (BAI)
SDIO/SDA*	General Electric (GE)
SDIO/SDT (NTBJPO)	MITRE Martin Marietta
USASDC	COLSA, INC.
NSA	SPARTA

* Government representative not available

The group has met on several occasions since its formation in March, 1991, to define and execute a methodology for development of a secure information transfer system for the NTB which includes the implementation and integration of the key enabling technologies of security, AIS interfaces, and communications and control.

The Tiger Team was formed as a logical successor to the NTB Security Strategy Working Group (NSSWG) which developed the security development methodology and produced a report which included a strawman architecture, and the guiding security policy for the NTB. The NSSWG provided a substantial step forward by identifying security as an enabling technology which must be integrated with AIS interfaces, communications and control in order to provide the infrastructure necessary to support the NTB mission. The Tiger Team has incorporated the products of the NSSWG work within its approach and has provided the necessary integration of these elements.

The Tiger Team has defined a top-down development approach to ensure compilation and integration of NTB mission requirements and timely development and implementation of a responsive NTBN architecture. The approach comprises four primary phases:

(1) Compile functional communications and security requirements based on examination of the NTB operational environment and on various users' and operator's perceptions of information transfer requirements to support the NTB mission;

(2) Compile applicable communications and security technologies that would support architecture definition;

(3) Develop a communications and security architecture and operational concept which builds upon the NSSWG work which has been done, and also incorporates consideration of the compiled requirements and available technologies; and

(4) Develop a phased implementation plan which provides a migration strategy for achieving the NTB security and communications goals.

The first two phases of the Tiger Team approach were executed concurrently by a requirements subgroup and a technology subgroup, each of which comprised a cross-section of the Tiger Team members. The results of the four phases are presented in this report.

C. <u>References</u>

(1) NTBN Draft Requirements Report, May 10, 1991

(2) NSSWG Draft Final Report, March 4, 1991

(3) DoD Directive 5200.28, Security Requirements for Automated Information Systems, March 21, 1988

(4) DoD Standard 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985

(5) National Computer Security Center Guidelines, NCSC-TG-XXX (also referred to as the "Rainbow Series")

II. WORKING DEFINITIONS

In order to provide the mechanism to ensure the consistent presentation of ideas, certain generally used terms were given strict definitions. These definitions are entirely consistent with those used by the NSSWG, and will continue to be used in all SCAWG efforts.

(1) National Test Bed (NTB)

The Automated Information Systems (AIS) equipment, and its environment, that is used to support the SDIO research and development (R&D) effort. The assets may be connected to the National Test Bed Network.

(2) NTB Network (NTBN)

The Communication and control medium that permits connection between NTB AIS assets. (It can also be thought of as being bounded by the last electronic connection of any NTB AIS that can communicate with other NTB AISs).

(3) NTBN Node

The AIS equipment and its environment at a particular physical location that is used to support the NTB and is connected to the NTBN. (e.g., the NTF or SDC).

(4) National Test Facility (NTF)

The AIS equipment, and its environment at Falcon Air Force Base, that is used to support the NTB (e.g., Computer Room 1 and Directed Energy Support Center, which are connected to the NTBN). (The NTF currently acts as the hub for NTBN communications.)

III. THE CHALLENGE AND COMPELLING NEED

The need for security in the NTB operational environment is dictated by the sensitivity of information and the internal and external threat of compromise of that information. Security as such is an enabling technology which provides a wide range of users access to shared computer and communication resources which process information at multiple levels of classification. The challenge in providing the needed security is defined by the environment within which the NTB mission must be performed. The key elements of the mission environment include:

(1) Dispersed geography with many AIS platforms and many requirements to communicate;

(2) A wide range of users from Government, industry, and various U.S. Allies; and

(3) A wide range of security classification levels required.

In order to accomplish the mission within this operational environment, certain fundamental components of infrastructure must be implemented in an integrated manner, and include communications and control, security, and AIS interfaces. These components provide the enabling technologies needed to support secure information exchange among the broad and dispersed NTB user community. The interaction among these components of infrastructure demands that an integrated approach be utilized in defining the system requirements and architecture.

IV. REQUIREMENTS

A. Technical Approach for Requirements

The derivation of the security and communications requirements was approached from a mission perspective as well as user (i.e. SDIO organizations and associated contractors that need secure communications services (NTBN) to perform experiments and testing) and operator (i.e. the builders and maintainers of the NTBN) perspectives. Examination of the mission drove the derivation of fundamental requirements for security and communications infrastructure, while the compilation of user and operator views of requirements either validated or refined the fundamental mission-driven requirements.

The approach for compiling user and operator perspectives of functional communications requirements involved two views: top-down and bottom-up. The top-down view consisted of asking managers in the SDIO community to identify current and potential future information transfer requirements to execute the various levels of tests required. The results of initial interviews to determine the high-level or top-down view of requirements were presented at the April 8-9 Tiger Team Meeting, and are contained in Annex 1. Concurrent with this effort, the Requirements Team investigated current NTBN utilization, assuming that current security and communications requirements offer a useful low-level or bottom-up view of future system requirements. The correlation of these top-down and bottom-up requirements provide a set of requirements data on which to base an architecture design. From the bottom-up view, the Requirements Team obtained current and projected NTF and SDC user requirements. From the top-down, two views were compiled: (1) user requirements were obtained through interviews with SDIO/SDN, SDG, and TD; and (2) GE provided the SEIC requirements perspective.

B. Expected Future Use of Data

In order to take full advantage of the requirements data gathered for this effort, an NTBN User Requirements Database has been created by SDIO/POI. This database contains all of the pertinent programmatic data derived from the raw data provided in Annex 1. Separate entries are made for each test function identified by NTBJPO and USASDC. Separate entries are made for each test concept identified by SEIC. All of these entries are called 'SDS Function' in the database. For each SDS Function, the following data are provided as available:

(1) User Organization;

(2) SDIO Sponsor (person);

(3) SDIO Sponsor Organization;

(4) Contract Number;

(5) Contract Type (i.e., system/subsystem/element; technology; or other);

(6) User Type (i.e., administrative data exchange; model development/batch simulations; or interactive, distributive or real-time simulations/experiments);

(7) Node;

(8) Data Rate; and

(9) Security Classification.

At a minimum, the database allows data to be sorted by sponsor organization, user type, data rate, and security classification. The database in aggregate form provides requirements information for initial architecture development. The database will be maintained with current data ensuring that the NTBN architecture evolution and implementation planning can be driven by requirements.

C. Consolidated NTBN Requirements

1. NTB Mission Guidance

The NTB mission and DoD security policy directly drive the general requirement for a security, communication, and AIS interface infrastructure. The original NTB Charter statement dated August 4, 1986 establishes the context for the infrastructure:

> "Provide the comprehensive capability to compare, evaluate, and test SDS architectures, key technologies, and BM/C^3 strategies."

Further direction by President Bush in late 1990 established another component direction to SDIO regarding the GPALS concept, and thus implied an added direction for the NTB. The NTB mission examined in light of the environment in which it must operate quickly identifies three important factors:

(1) The geographically dispersed nature of the SDI programs is also reflected in the dispersed nature of test resources and users and will continue to be so in the future;

(2) The sensitive and classified aspects of SDI technology and research must be protected from unauthorized access, modification, and destruction; and

(3) The NTB must operate in a common or shared user environment which includes participation by Government organizations, allied nations, and multiple contractors.

A restatement of these factors as a generalized infrastructure requirement follows: the NTB is required to provide testbed resources, protected from unauthorized use or intrusion, with user access across a broad geography for a variety of Government, contractor, and allied nation users.

2. System Functionality

In support of the SDI mission, the NTB goal is to provide a common test environment for the design of SDS, including:

(1) To support the simulation and validation of SDS elements and overall system concepts;

(2) To support the planning and conduct of system element and overall system studies and analyses that are excursions from the baseline SDS concept;

(3) To provide support to USSPACECOM for Concepts of Operations (CONOPS) and operational training;

(4) To support coordination of SDI field experiments involving multiple elements;

(5) To support establishment and maintenance of a state-of-the-art simulation and analysis capability including connectivity among NTBN nodes;

(6) To provide a data repository for all SDIO approved models, experiments, and simulations;

(7) To support configuration control of all SDS models software; and

(8) To collect, store, and provide access to standard SDI threat data.

3. System Requirements

The NTBN infrastructure must exhibit certain system security and communications characteristics in order to be responsive. The critical characteristics are flexibility (including growth capability), modularity, and standardization.

The requirement for flexibility is derived from both the changing mission environment and the evolution of test phases as cited by the SDIO user community. The mission environment is altered by the redirection of SDIO toward theater and tactical considerations which in turn may alter the required geographic dispersion of supporting NTB resources. The evolution of test phases as identified in interviews with SDIO/TD, SDN, and SDG indicate that most of the programs in SDIO are still in early stages of development, and as development progresses test complexity and scope will expand. New sites may be added, and must be accommodated by the NTBN.

The requirement for modularity follows the derivation of the requirement for flexibility, and the need to support a shared resource user community. With a dynamic user community accessing a shared resource, a common set of mechanisms for providing that access is essential for system responsiveness. A modular approach allows the system to easily adapt to varying data capacity and security requirements, making resources available as they are needed. Thus modularity is a critical characteristic that must be incorporated in a responsive system architecture.

The need for standardization (and conformance to a guiding set of standards) derives from the dynamic nature of the NTBN user community and from public law and DoD and federal policy. Standardization of security mechanisms, communications mechanisms, and operational procedures will be essential to maintaining a responsive NTBN over its life cycle. The selection of a guiding set of standards for the NTBN architecture is driven by this need for supportability and maintainability; however, it is also recognized that standards in communications and security are still evolving and thus the NTBN architecture must be flexible enough to evolve with those standards.

4. Security Requirements

Access to data on the NTB must be restricted to only those users who are appropriately authorized for that data. Authorizations shall be based on a user's security clearance, need-to-know, and restrictions resulting from organizational conflicts of interest. To meet the projected user requirements and to enhance the current capabilities, the NTB, and in particular the NTF and the NTBN, should support a Multilevel Secure (MLS) mode of operation. The MLS requirement is directly driven by the NTB system requirement to "provide a common test environment for the design of SDS", and by the wide participation of Government, academic, industry, and allied nation organizations.

This requirement statement is in general supported by the compiled user requirements which reflect many specific requirements to simultaneously process unclassified to Secret information and in a few cases Secret to Top Secret information.

5. Communications Requirements

The NTB user communications requirements assembled by the Tiger Team's requirements subgroup and presented in Annex 1 were examined in aggregate for trends which may influence the system architecture. Validation of these data through interviews with SDIO personnel could result in minor changes. However, the data are not expected to change enough to affect the general conclusions which were drawn from them. In addition to identifying overall trends in the requirements, the assembled data were sorted and consolidated with respect to four key categories influencing the NTBN architecture. These are: sponsor organization, user type, security classification, and communications requirements (size and/or type). Specific conclusions drawn from this consolidation of the requirements data are included in Annex 1.

The most obvious conclusion which can be drawn from examination of the requirements data is that there is a large and diverse community requiring access to NTB resources. Further, this diverse community requires NTB assets for performing many different types of functions with varying levels of security requirements and data rates. One also notes that requirements change (sometimes significantly) over time. All of these factors validate the system requirements of flexibility, modularity, and standardization outlined earlier.

The NTF, USASDC, and SEIC requirements data can also be assessed with regard to the High-Level User View of NTB communications requirements. The high level view was compiled through interviews within three broad categories in SDIO: Strategic Defense Deputate (SD) other than Brilliant Pebbles, Theater Missile Defense Deputate (TD), and Brilliant Pebbles (BP) activities. The compilation of these user views indicate that there are three general areas of communication requirements for support of SDS or GPALS tests and experiments:

(1) Simulation to simulation communications, primarily within a single node;

(2) Simulation to prototype communications across a broad geography; and

(3) Prototype to prototype communications across a broad geography.

Common to all of these general communications requirements is the need to provide access to a wide range of test participants and users. The first category of communications requirement indicates the need for local node communications throughput which may exceed tens of megabits per second, depending on simulation approach. The next two categories indicate an extension of this throughput requirement to internode communications sometime in the future. It should be noted that the definition of these requirements was at a more advanced stage at SD than within TD or BP.

In general, it appears that the requirements identified in this effort represent current and near-term future requirements, which explains why they in large part represent non-Theater Missile Defense (TMD) and non-Brilliant Pebbles functions. This conclusion further emphasizes the dynamic nature of the NTB communications requirements, and thus the need for a flexible and modular architecture, as well as the need to complete and maintain the database of user requirements.

The consolidated requirements data show a large concentration of NTBN user requirements originating from the SD, but with all current internode throughput requirements at T1 rate or less. As these data are validated, and as TD user requirements are defined, however, both the size and origin of NTBN user requirements could change significantly. Thus it is essential that the NTBN have a modular architecture to allow for modular growth.

V. ENABLING TECHNOLOGY

This section provides an introduction to the technologies and products which provide the basis for implementing systems meeting the requirements defined in Section IV. Additional information on the security and communications concepts introduced below may be found in the NSSWG Final Report. Definitions of terms may be found in the glossary and are consistent with those given in the National Computer Security Center's (NCSC's) "Rainbow Series" of publications. Additional data on available products is presented in Annex 2 of this report.

A. Security and Communications Concepts

The material in this paragraph is presented as background to assist the reader in understanding subsequent discussions of technologies, products, and system architectures. Figure V-1 is a generic architecture diagram showing multiple nodes interconnected by a communications network. The node defined in Figure V-1 is a combination of hosts and LANs located at a specific site and connected to other nodes via a WAN. Figure V-2 identifies four categories of hardware/software products used in the generic network architecture. Definitions, examples and security concepts for these four product categories are presented below. Examples of product categories and security concepts are drawn from the existing NTBN architecture.

1. Host Computers

A host is any computer-based system connected to the network and containing the necessary protocol interpreter software to initiate network access and carry out information exchange across the network. This definition encompasses typical "mainframe" hosts, generic terminal support machines, and workstations connected directly to the communications subnetwork and executing the intercomputer networking protocols. A dumb terminal is not a host because it does not contain the protocol needed to perform information exchange; a workstation is a host because it does have such capability.

Examples of host computers on the existing NTBN include the CRAY, VAX and IBM mainframes connected to the classified network at the NTF and the SUN workstations which provide access to these NTF resources from each NTBN node. All hosts connected to the NTBN are currently accredited to process data at a single classification level (SECRET) in the Dedicated mode of operations (see Appendix C - Glossary for definition). Security features currently required for NTBN hosts are identification and authentication measures and limited audit capabilities. As part of ongoing efforts to upgrade selected host processors to System High accreditation, operating system software evaluated by the NCSC at the C2 (or better) level or containing equivalent features is being installed.

2. LAN Components

A Local Area Network includes the cable plant, interface electronics and associated software required to provide network services to LAN users in a single building or group of buildings connected primarily by local (i.e. not long-distance) communications circuits. Figure V-3 shows that each of ten NTBN nodes has an Ethernet LAN which connects to the NTBN WAN via an AIS integration component. Some nodes (e.g. SDC, ESD) have additional LANs connected to the NTBN via AIS Integration Components. Protected cable distribution systems are the only security feature currently associated with NTBN LAN components. Hosts connected to the LAN are required to have identification and authentication measures and audit capabilities. The existing LAN interface components have no evaluated security features and therefore limit the LAN to the dedicated mode of operation.

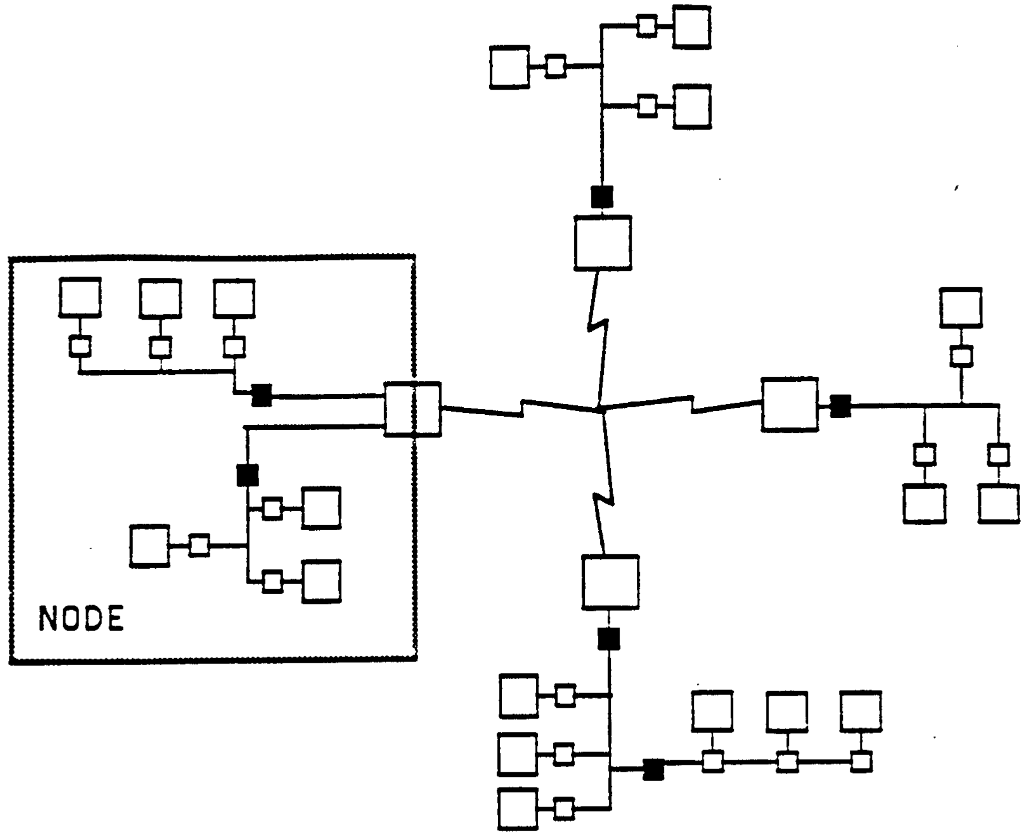


Figure V-1. Generic Architecture Diagram Showing WAN Nodes

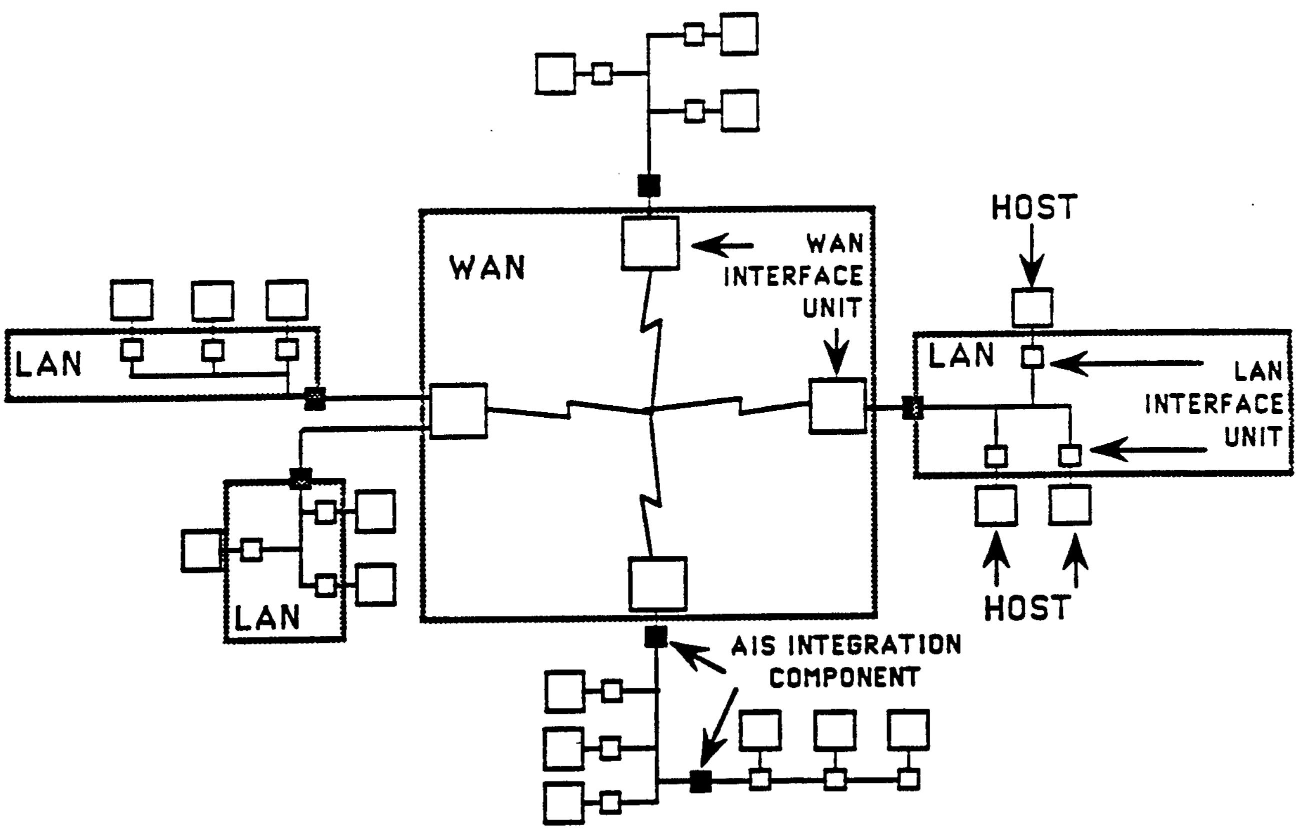


Figure V-2. Building Blocks for Network Architecture

NTBN ARCHITECTURE

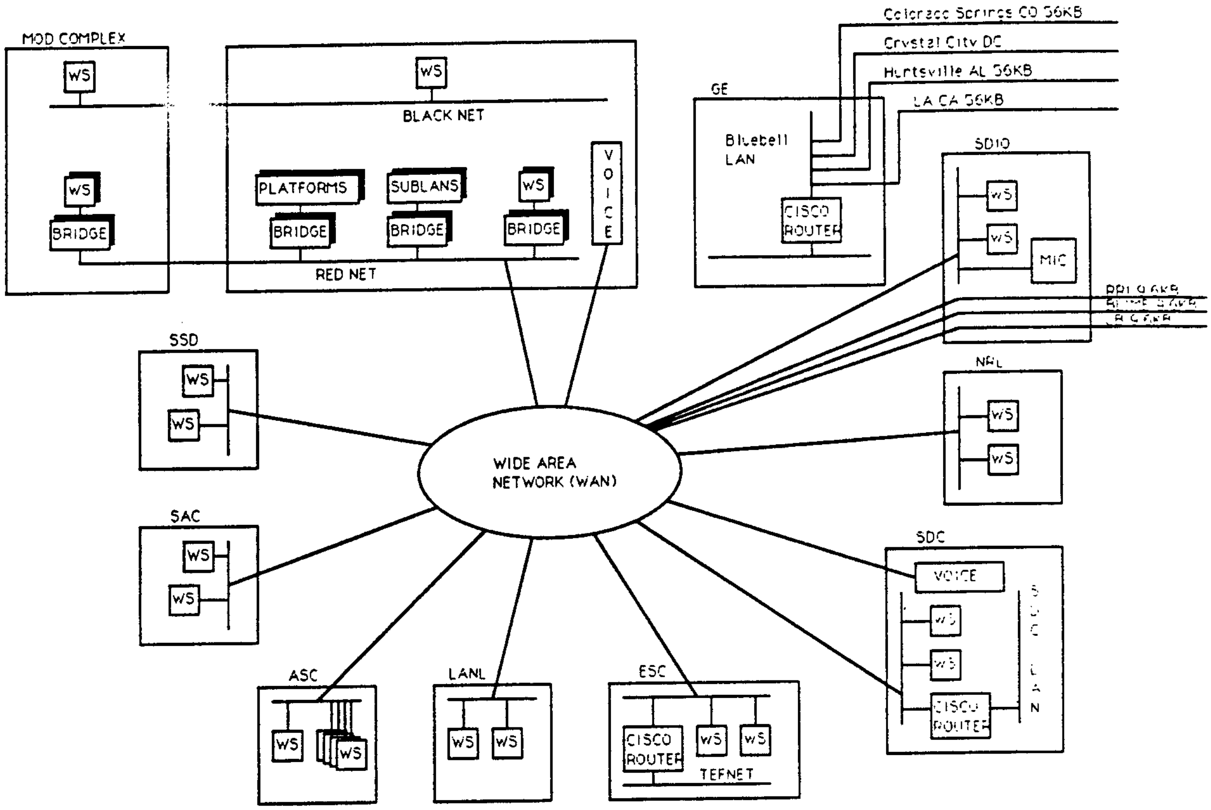


Figure V-4. Existing AIS Components At NTBN Nodes

NTBN WAN

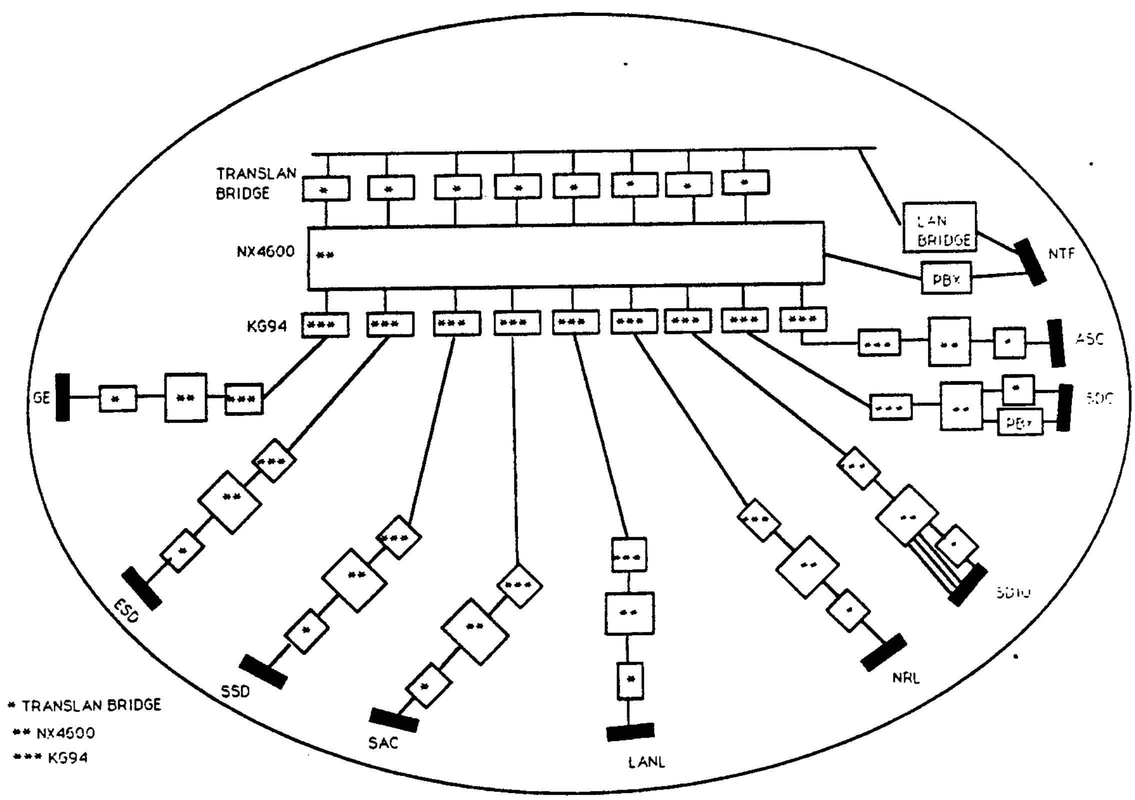


Figure V-4. Existing NTBN Wide Area Network

3. WAN Components

A Wide Area Network includes the cable plant, interface electronics and associated software required to provide network services to users distributed over a wide area and connected by long-haul communications circuits. For the existing NTBN, the intelligent switches (NX4600s), link encryption devices (KG-94s), and T1 communications circuits shown in Figure V-4 are WAN components. The only security feature associated with existing NTBN WAN components is the Type 1 encryption provided by the KG-94s on the dedicated point-to-point communications circuits between nodes. These WAN components do not provide any security features which would permit the WAN to operate above the dedicated mode.

4. AIS Integration Components

AIS Integration Components include devices such as gateways, guards, bridges, and routers which allow users on one LAN to access resources on another LAN or on different segments of the same LAN. These components appear at the boundaries between the LANs, WANs and hosts identified in Figure V-2. They provide the "glue" which binds separate AISs into an integrated network. The following AIS Integration Components have potential application to the NTBN architecture:

(1) Guard. A processor which provides a filter between two disparate systems operating at different security levels or between a user terminal and a database to filter out data that the user is not authorized to access.

(2) Bridge. A device which interconnects LANs and which may restrict packets to a local segment of a larger network for performance reasons. As shown in Figure V-3, bridges are used at the NTF to connect the primary node LAN to other LAN segments on which NTF hosts are installed.

(3) Router or gateway. A device which selects the optimal route to send traffic over a network and may restrict traffic to or from a LAN for performance reasons. Unlike bridges, routers work in conjunction with specified network protocols such as Internet Protocol (IP). As shown in Figure V-3, routers are used at various nodes to extend the local Ethernet to a remote location. The functions of a bridge and router are often combined in a single product.

The AIS integration components currently in use on the NTBN have not been evaluated for compliance with NCSC computer security guidelines. Therefore, the network has not been accredited to operate beyond the dedicated mode.

B. Overview of Secure Networking Product Technologies

As described above, products with potential applications to NTBN communications and security upgrades may be grouped into four categories--Host Computers, LAN Components, WAN Components, and AIS Integration Components. The choice of products within each category is driven by performance and security requirements. For networks such as the existing NTBN operating in the Dedicated mode, no minimum level of trust is required by the governing DoD standards (NCSC Rainbow Series publications), and products may be selected without regard to their NCSC certification level. NCSC guidelines recommend products with a Trusted Computing Base (TCB) evaluated at the C2 level for System High applications, at the B1 level for Compartmented mode applications, and at the A or B2 level for Multilevel mode applications. Type 1 encryption is a requirement for all networks which transmit classified data over unprotected distribution systems.

Table V-1 is a summary of the products surveyed during the preparation of this report. It includes products which are currently available as well as products now under development. The columns in Table V-1 are the four product categories defined in paragraph A above. The rows are based on a further categorization of products as defined below:

(1) Evaluated Products List (EPL) Products. Hardware/software products listed on the NCSC's Evaluated Products List (EPL) in one of four phases of evaluation (Vendor Assistance Phase, Design Analysis Phase, Formal Evaluation Phase, and Completed Evaluations). The EPL groups products functionally into four types--Unix-like Systems, Proprietary Systems, Networks and Network Components, and Subsystems. The Unix-like and Proprietary Systems are computer platforms with secure operating systems which are evaluated with respect to the NCSC Trusted Computer System Evaluation Criteria (Orange Book). They appear in Table V-1 under the Host Computer column. It should be noted that some of these systems have been configured in network applications as gateways and guards, and therefore they also appear under the AIS Integration Component column of Table V-1. The EPL Network and Network Components products are evaluated in accordance with the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (Red Book). EPL Subsystem Products are those which have been evaluated with respect to Orange Book criteria, but do not meet full system requirements for A, B or C-level evaluation.

(2) Computer Security (COMPUSEC) Products Not on EPL. Hardware/software products which have been designed to meet NCSC standards or which include some computer security features, but which do not currently appear on the EPL under any of the four evaluation stages. Examples are the BLACKER network components developed by NSA for X.25 WAN applications and the TimeLAN 100 FDDI LAN developed by Unisys.

(3) Communications Security (COMSEC) Products. Devices which provide Type 1 encryption at the Host, LAN or WAN level. Two products listed in Table V-1, BLACKER and CANEWARE, incorporate both COMSEC and COMPUSEC.

(4) Other Products. Commercial products which provide neither computer security nor Type 1 encryption capabilities. They are listed in Table V-1 because there are many applications in a secure network for products which incorporate neither COMSEC nor COMPUSEC features. One example is a single-level hosts or LAN which is connected to an MLS network by an AIS Integration Component with an appropriate TCB. Another example is a WAN communications component such as a packet switch located on the BLACK side of the WAN COMSEC device.

The Tiger Team drew two important conclusions from its survey of available networking products. First, members agreed that products are available today to integrate a first generation MLS capability for the NTBN. Second, the Tiger Team concluded that an MLS network meeting NTBN requirements cannot now be assembled from the small set of products which have successfully completed NCSC evaluation. Products from each of the four categories defined above must be considered for the near-term MLS implementation. The Tiger Team also concluded that it may be necessary to work with vendors to define enhancements which will bring existing products into compliance with NTBN requirements. The Architecture discussions in the following sections provide guidance on integrating the secure networking products and technologies introduced in this section into the NTBN to achieve a multilevel secure network. The guiding criteria in selecting products will be interoperability requirements (i.e., compliance with DoD protocol standards) and performance requirements (i.e., data transfer speeds consistent with those on the existing network).

TABLE V-1
SUMMARY OF APPLICABLE PRODUCTS

DESCRIPTION OF PRODUCTS	PRODUCT CATEGORIES			
	HOST COMPUTERS	LAN COMPONENTS	WAN COMPONENTS	AIS INTEGRATION COMPONENTS
EPL PRODUCTS	UNIX-like Systems (16 EPL Products)	Verdix VSLAN (Completed Evaluation at B2 Level)		Loral MLS-100 Gateway (Vendor Assistance Phase-B2)
	Proprietary Systems (23 EPL Products)	Boeing MLS LAN (Formal Evaluation Phase for A1 Level)		UNIX-like and Proprietary Syst. Configured as Guards/Gateways (Examples are the HFSI XTS-200 and the Gemini GEMSOS Guard)
	Evaluated Subsystems Meeting Selected COMPUSEC rqmts.	Gemini Network Processor (Design Analysis Phase for A1 Level)		
COMPUSEC PRODUCTS NOT ON EPL		Unisys TimeLan 100 FDDI LAN	BLACKER Front End (Designed to A1 Standards)	Verdix Secure IP Router (EPL Application Pending)
		DEC DESNC Secure Ethernet LAN	CANEWARE (Designed to B2 Standards)	DEC One Way Gateway
COMSEC PRODUCTS (TYPE 1)		Motorola NES Products	Motorola NES Products	
		Xerox XEU (Link Encryption Device)	Xerox XEU (Link Encryption Device)	
		Wang TIU (Link Encryption Device)	Wang TIU (Link Encryption Device)	
			BLACKER Front End (X.25 Network Encryption Device)	
			CANEWARE (SDNS Encryption Device)	
			STU-III and KG-Link Encryption Devices	
OTHER PRODUCTS (NOT COMPUSEC OR COMSEC)	Commercial Host Platforms	Commercial LANs	Packet Switching Products	Commercial Protocol Converters
			Intelligent Data PBXs	Commercial Router Gateway and Products
				Commercial Bridge Products

VI. SYSTEM DESCRIPT`ON

The NTBN security and communications architecture system description contains two essential areas:

(1) An NTBN operational concept, and

(2) NTBN security architecture.

The operational concept details the communications and security management considerations for the NTBN. The architecture section provides a description of alternative approaches to providing a secure and responsive NTBN, and proposes a recommended NTBN communications and security architecture.

A. Operational Concept

The communications and security policy for the NTBN shall be considered throughout the life cycle of the Automated Information System (AISs) and the network from beginning of concept, through design, development, operation, and maintenance. The cycle should ensure early and continuous involvement of the users, information system security officers, data owners, and Designated Approving Authority (DAA) in defining and implementing the security requirements of the AISs. The DAA is the person designated as responsible for the overall security of AISs and networks for a major command or agency. This operational concept for the NTBN security and communications architecture covers organizational management, network security management, configuration management, cryptographic management, risk management, and operational test and evaluation.

1. Organizational Management

The NTBN crosses a myriad of DAA boundaries when network connections are provided to various Government agencies and contractors. Although the Strategic Defense Initiative Organization (SDIO) has authority over the NTBN, there are several other command and agency DAA's that have control over their respective AISs. Currently the list of DAA's includes United States Army Strategic Defense Command (USASDC), Department of the Energy (DOE), US Space Command (USSPACCOM), Naval Research Laboratory (NRL), Strategic Air Command (SAC), Defense Investigative Service (DIS) and Space Systems Division (SSD). The SDIO shall develop agreements with these organizations and any future organizations at the policy level and the operational level relative to security of the NTBN and respective AISs.

a. DAA Memorandum of Agreement (MOA)

The NTBN is a network of AISs previously accredited by their respective command DAA. DoD Directive (DoDD) 5200.28 states that if the network consists of previously accredited AISs, an MOA is required between the DAA of each DoD Component AIS and the DAA responsible for the network, SDIO. The memorandum of agreement between DAAs must recognize each DAA's scope of responsibilities, encompass the security policies and practices of each DAA, and other information included in DoDD 5200.28 Paragraph D. The MOA should reconcile different security policies and philosophies of protection and identify the conditions under which specified classes of information can be exchanged. The security of each AIS connected to the network remains the responsibility of its individual DAA. The DAA responsible for the overall security of the network, SDIO, shall determine the security and protection requirements for connection of AISs to the network and have the authority and responsibility to remove from the network any AIS not adhering to the security requirements of the network. Each MOA should also outline how the DAAs deal with security issues and how to resolve any differences. The following

is a list of recommendations for the contents of the MOA and supporting documents taken from the Trusted Network Interpretation guideline:

(1) A general description of the information that will be transmitted to the network by each AIS.

(2) A summary discussion of the trusted behavior that is expected from each AIS.

(3) The details of the overall security plan for the network and the assignment of responsibility for producing and accepting the plan.

(4) A description of the overall network security policy.

(5) Specification of the security parameters that are to be transmitted between communicating AISs

(6) A discussion of security details that are relevant to the exchange of information among the AISs.

(7) A description of the user community, including the lowest clearance of any user who will have access to the network.

(8) Any special considerations for connections to any AIS in the network, including potential security threats and the safeguards that will be used.

(9) A description of the security protection features provided by the data communications and network security control devices.

(10) A description of the information that each AIS will log in the audit trail and how auditing tasks will be divided among AISs.

(11) A description of the information security services to be offered to the network by each AIS.

b. Intersite MOA

The operational computer sites that are nodes of NTBN and the NTBN manager should establish MOAs to cover the various operational security aspects of the DAA MOAs. These MOAs should establish how controlling mechanisms are employed and establish reporting procedures for security requirements, modifications and incidents.

2. Network Security Management

a. Access Control

The network access control mechanisms must enforce the network security policy. The network must control access to network resources based on classification level (MAC [mandatory access control]) and need-to-know (DAC [discretionary access control]). In this way, data transmission and reception across the network will be mediated by the network and only those resources with the correct clearance and/or need-to-know will be able to communicate. The network must be able to authenticate the identity of its attached computers to ensure correct knowledge of classification levels.

Network access control can be accomplished by the use of separate networks for each classification level processed or by use of multilevel secure (MLS) network devices.

b. Audit

The audit mechanism of a network has five important goals. First, the audit must allow the review of patterns of access to individual systems. Second, the audit mechanism must allow the discovery of both user and outsider attempts to bypass protection mechanisms. Third, the audit mechanism must allow discovery of any use of privilege that may occur on the network. Fourth, the audit mechanism must act as a deterrent against perpetrators habitual attempts to bypass the system protection. Finally, the audit mechanism must supply assurance that attempts to bypass the network security mechanisms will be recorded and discovered.

c. Intrusion Detection

The network should provide a means to automatically discover any attempts to bypass network security controls or to discover any actual breach of network security.

Audit mechanisms collect massive amounts of information regarding the security operation of the network. An intrusion detection system is needed to analyze the audit log(s) to allow the Network Security Officer (NSO) to obtain data on the secure operation of the network. A real-time intrusion detection system is highly desired. This type of system would be able to analyze network audit logs, in real-time, and determine if security anomalies are occurring. A non-real-time system, which is less desirable, would perform post-processing of audit data and would still be invaluable to the NSO who would not have to examine voluminous audit logs with the high potentiality of missing security anomalies.

d. Configuration Management

A formal network configuration control board (NCCB) for the NTBN should be established. This NCCB should establish procedures for changes to the network, review proposed changes and pass recommendations to the DAA where network security would be affected. Configuration management procedures identify the configuration of a network at discrete points in time for the purpose of systematically controlling changes and maintaining integrity and traceability of this configuration throughout the network life cycle. Configuration management consists of identification, control, status accounting and auditing.

(1) Identification is to identify the components of the network design and the implementation.

(2) Control involves the systematic evaluation, coordination, approval/disapproval of proposed changes to the design.

(3) Status accounting is to record and report all information that is of significance to the configuration management process.

(4) Audit is checking the top to bottom completeness of the configuration to ascertain that only authorized changes have been made in the network hardware, software or firmware.

e. Cryptographic Management

To provide data confidentially and integrity, as well as network control integrity, NSA Type 1 cryptographic devices must be used on all network communications circuits that are not security controlled (e.g., not in secure spaces or protected wire-line distribution systems). In addition, encryption can be used to provide data privacy and separation of classification communities.

f. Risk Management

No security system is perfect. The risk remaining in a proposed AIS must be assessed and if found to be acceptable to the DAA, granted accreditation. All AISs must be accredited before they may process or use classified information, unless a written waiver is granted by the DAA. The accreditation of an AIS is based upon a technical investigation and a formal review in accordance with DoD 5200.28. The DAA must ensure that satisfactory security measures have been installed and that any residual risk is within acceptable limits which must be weighed against operational necessity.

DoD 5200.28 (enclosure 4) states that the risk assessment method for evaluating AISs will be the procedure based upon CSC-STD-003-85, the "Yellow Book." Any DoD component desiring to use a different method to accomplish the intent of the 5200.28 may do so only with prior approval granted by ASD (C3I). DoD 5200.28 does not define accreditation requirements for non-DoD AISs or for connecting non-DoD AISs to DoD systems. An alternative to the Yellow Book method has been developed by the Naval Research Laboratory. The Yellow Book takes the high level view of the system risk whereas the NRL paper includes several more detailed aspects of the system processing. The NRL methodology encompasses all of the Yellow Book's methodology, but because of its finer granularity, may be more applicable for use in the NTB environment. The NRL methodology provides a more in-depth risk analysis and could result in a more precise set of requirements based on the environmental usage of the system. This method warrants fuller investigation in coordination with ASD (C^3I).

SDIO Manual 5206 requires an annual accreditation review for each AIS. An accreditation review consists of an inspection of an AIS or network, its capabilities, and its physical facilities to include the following activities: 1) reevaluation of the need for accreditation at the current sensitivity level; 2) evaluation of the current accreditation; 3) determination of problem areas or unresolved issues; and 4) determination of the adequacy of the implementation of the security approach. These reviews should be conducted by personnel independent of the AIS or network staff. A successful accreditation review indicates that the previous accreditation is still valid. Otherwise, the accreditation process defined in SDIO Manual 5206-M must be initiated.

After initial DAA accreditation, the risk management is a recurring process and must correlate with network configuration control. Each time a network configuration change is proposed, a risk assessment must be accomplished to determine potential impacts on current acceptable risks. Network changes must be viewed in relation to the current existing network to ensure no new risks are introduced. SDIO Manual 5206-M defines the types of changes which require coordination with the SDIO DAA prior to implementation of the changes.

g. Operational Test and Evaluation

Network security mechanisms must work correctly because they are relied upon to provide network protection against security bypass resulting in security compromise. In addition, distributed security mechanisms must interoperate with one another to provide network security.

In order to ensure that the security mechanisms work correctly, assurance of correct operation must be provided. The assurance is a result of design and implementation evaluation and/or verification. Evaluation and verification can be done in a formal, mathematical manner (using predicate calculus analysis), by exhaustive operational testing, or both. The secure interoperation of network components must be shown to work correctly.

There must be continual testing of security enforcement mechanisms throughout the operational life-cycle of the network to assure continued secure operations. This testing could use both off-line and on-line methods. In an off-line fashion, network components and systems could be removed from the active, operational network and installed on an off-line, non-operational test network. Under the direction of the network security manager (NSM), tests would be implemented to attempt to bypass the component's network security features and mechanisms. To prove that the component was operating securely, not only should the bypass tests fail, but the fact that the tests were attempted should appear in the network audit log and should be exposed as possible attempts to breach security by the intrusion detection system.

These same types of tests could be run in an on-line fashion, but only with the strict advice, consent, and supervision of all of the cognizant network security authorities responsible for the network's secure operation. Tests performed on an operational network may cause undesirable side-effects such as disruption of network services. Therefore, users should be warned that such tests are to be undertaken, or the testing should be performed at non-critical or off-peak utilization times (i.e., midnight to 8:00 a.m.).

B. Architecture

1. Introduction

In defining a responsive NTBN communications and security architecture, a comprehensive examination of feasible architectural alternatives was conducted. The architectural alternatives were driven by the compiled functional requirements. The global set of alternatives may be categorized within two areas: (1) multiple, single level networks (Figure VI-1), or (2) a single, multilevel secure network (Figure VI-2). Given that the NTB has requirements to provide processing and data storage for users who are not all cleared to the same classification level, the NTBN must provide assured separation of user data on the network. This can be provided for by either of the two types of architectures. The overall tradeoff of the two architectures is driven by responsiveness and cost.

The NTB's current configuration consists of several independent networks. Some networks are unclassified; the others operate either in a Dedicated or System High mode with users cleared to the highest level of data processed on the network. The requirements analysis documented in Annex 1 of this report supports the need for several more single-level networks in order to serve the needs of the NTB's users.

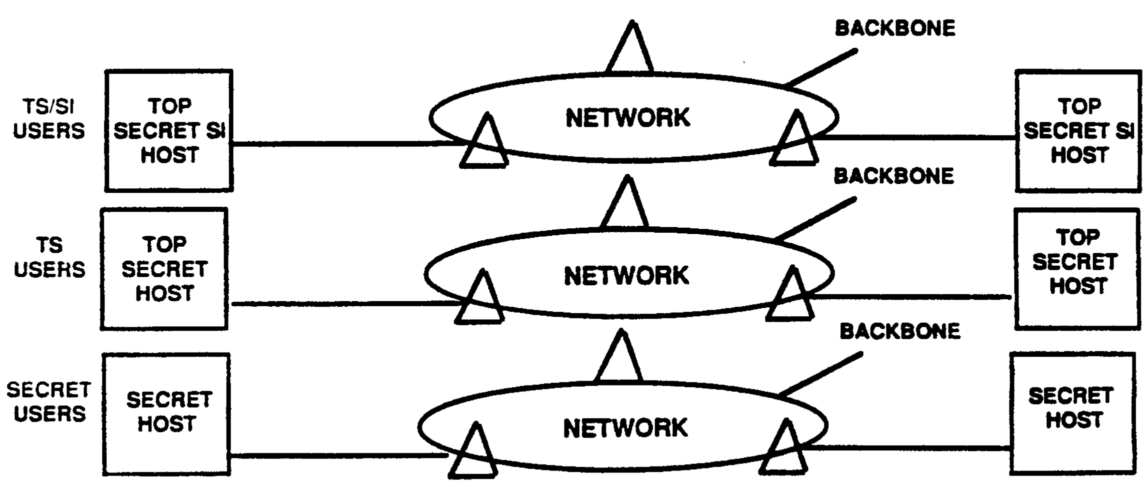


Figure VI-1. Separate Single Level Networks

As an alternative to the proliferation of multiple, single level networks, a single, multilevel secure (MLS) network could be employed to support the NTB users. The MLS network architecture could use a single network backbone to provide services to users with varying security clearance levels and computers with data of varying levels of classification.

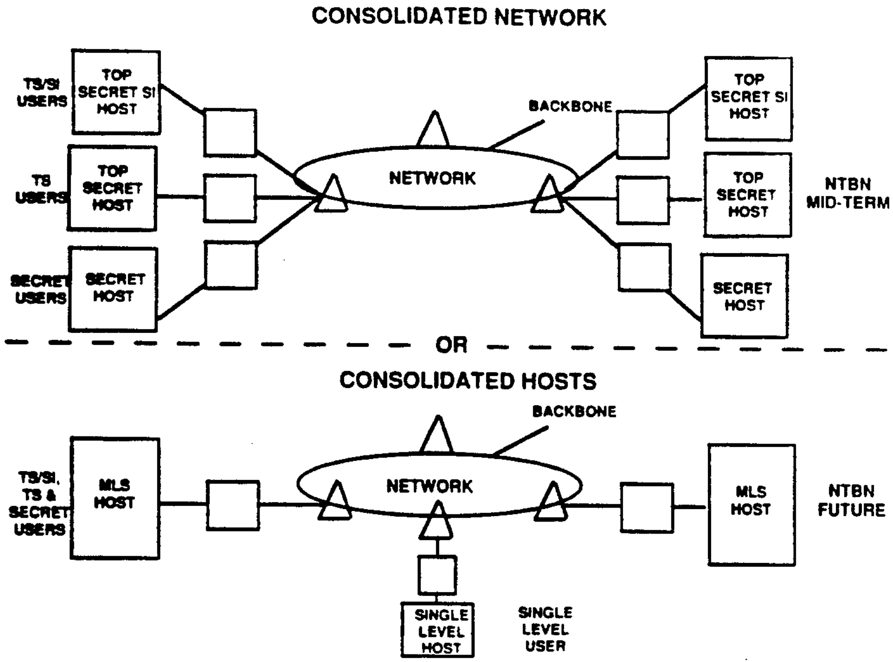


Figure VI-2. Single Multilevel Networks

A priority of providing additional NTB security functionality is to do so with the provision of working within the framework of network standards, whether they be domestic (DoD, GOSIP) or international (ISO/OSI). From a cost standpoint, as well as an interoperability standpoint, a heterogeneous and multivendor network is most desirable. As more standardized secure products make their way into the marketplace, the NTBN can incorporate these equipments to upgrade network security. This will allow the NTBN to reap the benefits of new technology as advancements are made by system vendors. For these reasons, a potential proprietary solution to the NTB MLS problem was not favorably accepted by the Tiger Team due to the overriding reliance on a particular vendor's technology solution(s), equipment(s), and communications protocols. The computer and network world, as it is seen today, is one that is quickly migrating to open systems standards.

2. Strawman Architectures

As stated in the previous section, the two major architectural designs that can be utilized to provide overall network system security for the NTB are multiple, single level networks, and a single, MLS network. From a high level perspective, these networks can be considered "back-bone" networks - that is, networks that transport data from source to destination without regard to the actual underlying technology that provides the data movement. In fact, from the user's perspective, it does not matter whether the underlying back-bone network is copper cable or fiber optic, or whether it is considered a local area network (LAN) or a wide area network (WAN). The distinction between LAN and WAN has become blurred in recent years because both technologies are being used in complimentary architectures, or in architectures that had once been the other's exclusive domain.

Most, if not all, modern networking systems employ a technology known as packetization of data. This means that the data traversing the network is grouped into packets

(or frames) of a finite size of bits (which may vary among network system implementations and may also be dynamic within a network), with each packet having an individual header typically denoting where the packet came from and where it is going to (i.e., its source and destination).

As a result of the basic research carried out in the late 1960s which resulted in the ARPANET, packetized data was routed from its source to its destination via a technology known as "packet switching." Packet switching implies that there are store and forward packet switching nodes which make routing decisions based on a knowledge of the network topology. The packet switching nodes forward the packets to a neighboring switching node in order to deliver the packet to its final destination. Until the advent of the ubiquitous local area network (such as Ethernet/IEEE 802.3), basically all packet network systems were packet switching systems.

Network systems which employ a bus (i.e., IEEE 802.3/Ethernet) or ring technology (i.e., IEEE 802.5/IBM Token Ring) differ from those that employ packet switches in that the bus or ring systems do not switch or route packets. The packets are broadcast on the transmission medium with source and destination addresses. All systems attached to the network read all the packets "flying" across the network. The attached system reads the packet header to determine if the packet is designated for itself. If it is, the packet is passed up to its intended application. If it is destined for another system, the packet is discarded.

There are many network security problems that network implementors are faced with. In the forefront, is the issue of data confidentiality. In a network environment, data is passed between computer systems via a physical medium. Most of those physical media are tappable or interceptable. This means that all the data that flows across the "wires" (whether they really be copper wires, fiber, or RF) is in danger of being read or modified in transit. The modification of data brings up the issue of data integrity. The recipient of the data needs to know how reliable the data is - for example, is the data that was received the data that was actually sent and was it sent by whom it says it was sent by. The question of authenticity of the source of the data implies that there is the possibility that someone other than the legitimate data source could masquerade as that legitimate source and possibly spoof the data recipient into performing actions that were unwarranted.

Interconnection of network components also presents a problem when those components are operating on data that needs to be protected differently. For example, one host may process and store data at the secret level, while another host might process and store data at the unclassified level. If there were uncleared users on the unclassified machine, the two systems could not be connected because there would be the possibility that uncleared users could obtain classified data. Only if the hosts or a network interface supported multilevel operations, could these two systems be connected with uncleared users. In many instances, the resultant segregation of systems causes a loss of system functionality because there may be a mission requirement to move data from an unclassified system to a classified system. Currently, security policies would prohibit such a connection unless appropriate (i.e., trusted) safeguards were employed.

a. Multiple Single Level Networks

In order to support users who are not cleared to the highest clearance level of data being processed or stored on NTB computing equipment, the NTB network architecture must enforce user separation so that those users will not be able to access data or processors at classification levels higher than their clearance level. One method of providing this separation is to provide each clearance level of users with their own set of network resources - separate network cable plant, network operations and control, and computing facilities to process and store data.

It has been shown by the user requirements database (ref. Annex A - Requirements Database) that there is a need for NTB processing at the following levels: Unclassified, Secret, Secret with compartments, Secret with company proprietary, Secret without any NOFORN data, and Top Secret. This would require the use of at least six separate sets of computing and communications resources within the framework of the NTB.

It is not clear that all the replicated levels would require a total duplication of hardware resources, but it could be expected that at least several of the levels would require major supercomputer or mainframe investments (e.g., Secret, Secret with compartments, Secret with company proprietary, Secret without NOFORN, and Top Secret all might require continual usage of a CRAY supercomputer for simulations along with communications networking components). If CRAY supercomputers were required on all of the networks, despite the fact that there was excess capacity on each of the CRAYs, the cost would be astronomical (e.g., six systems at approximately $15 million per system, resulting in a $90 million dollar investment). The excess capacity of each of the machines could not be used by another classification environment because of the potential for security compromise. Each separate network would also require additional computational systems such as file servers, workstations, terminals, printers, and network hardware (routers, bridges, taps, cable, etc.)

Overall, the multiple, single level networks are simpler to understand and their security mechanisms are much less complex than the single, MLS network. They are secure and fully meet the NTB's need for separation of users and data based on clearance and classification. On the other hand, there is a very high cost in replicating the hardware, software, administrative personnel, operations personnel, and support personnel for each security level environment.

b. Single, Multilevel Secure Network

Instead of multiple, single level networks, the NTB could employ a single, multilevel secure network. Such a network could be built using several commercial products that have either been or are being evaluated by the National Computer Security Center (NCSC) for use in multilevel secure environments.

Using such MLS products, single level or multilevel computing resources (e.g., supercomputers, mainframes, workstations, PCs, terminals) could be connected to MLS network interface devices. These interface devices would be initiated and controlled by a Network System Security Officer from a Network Security Controller console station. The MLS network interface device would be instructed by the NSO whether to treat an attached computer as single or multilevel. If the computer were to be treated as a single level resource, the specific classification level would be indicated (e.g., Secret, Top Secret). The MLS network interface devices would then be responsible for attaching the correct security label to all data transmitted from the attached computer. It would also be responsible for ensuring that any data received from the network is labeled exactly the same as the indicated classification level of the attached computer. Otherwise, the received data will not be forwarded to the computer and this event should be audited.

If a multilevel device is defined by the NSO, then the MLS network interface device would be defined to transmit and receive data within a specific range of classification levels. For example, a multilevel secure computer might be allowed to process data in the range of Secret to Top Secret. Therefore, any data that does not fall within that range would not be passed through the MLS network interface device. The MLS network interface device would be responsible for checking the level of the data as labeled by the MLS computer to ensure that the data is correctly labeled within the specified range. Any violations of security classification would be audited by the MLS network interface device. These audit notification would then be

examined by the network system security officer and/or an audit intrusion detection system to provide security alerts.

The MLS network interface devices could be designed for use on local area networks (e.g., Ethernet, Token Ring, FDDI), or could be designed for wide area networks (e.g., X.25, DDN, frame relay, ISDN, MAN). The major difference would be in the network access speed that would be required by the network interface device. Segments of the overall network would be interconnected using secure routers/gateways, bridges, and communications security (COMSEC) devices.

The major costs that would be incurred would be the procurement of the MLS network interface device components and the MLS network security controller. One MLS network interface device might have to be purchased for each computing resource attached to the MLS network backbone which could be relatively expensive. On the other hand, computers could be clustered into communities of interest or separate single-level systems, and each of these clusters could then be gatewayed onto the MLS network through an MLS network interface device. This might be cheaper, from an initial hardware investment standpoint, but with greater usage of MLS network components (or through large quantity discount purchases), the prices of MLS network interface devices can be expected to drop dramatically over the next few years.

Single level computer systems might still have to be housed in separate facilities until such time that they are able to be run in multilevel secure mode. But, network operations personnel would not have to be replicated. There would be a need for additional security personnel to ensure correct network operations, but the numbers involved would not be as great as the numbers necessary for the many replicated networks.

c. Comparative Analysis

Following a thorough review of the technology options available for meeting NTBN communications and security requirements, the Tiger Team concluded that establishment of MLS networks is now a realistic alternative to the continued proliferation of the single-level networks. The decision to recommend an MLS NTBN architecture was driven by several key factors. First, it will be prohibitively expensive over the long term to duplicate communications and processing systems for NTBN users at all the classification levels for which test bed services will be required. Second, single-level networks cannot efficiently support the future operational needs of the diverse SDI user community. Finally, the components of a first-generation MLS network are now commercially available as a result of recent industry and Government-sponsored product development and certification efforts.

Appendix A of this report summarizes the Tiger Team's evaluation of the following three alternative architectures for a multilevel secure NTBN:

(1) Architecture 1. This approach uses secure routers to connect MLS LANs to a communications network secured by link encryption devices. The MLS LANs use commercially available network interface units and control processors to meet requirements of the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria published by the National Computer Security Center (NCSC).

(2) Architecture 2. This approach employs the Government-developed BLACKER Front End (BFE) or CANEWARE Front End (CFE) devices as the interface between single-level LANs (or hosts) and a packet switched network. BFE and CFE systems provide Type 1 encryption as well as computer security features meeting the NCSC criteria for trusted networks.

(3) Architecture 3. This approach combines the security and communications features of Architecture 1 and Architecture 2. BFE/CFE devices provide a packet switched network interface for MLS LANs as well as single-level LANs, and routers provide a point-to-point interfaces between MLS LANs.

Candidate architectures were evaluated on the basis of their security features, performance, compliance with networking standards, and cost. A summary of this evaluation is provided in Figure VI-3. Specific technical evaluation criteria included the level of NCSC evaluation achieved by products used in the architecture, the communications throughput capability, and the level of compliance with DoD standard protocols. The Tiger Team ruled out architectures based on proprietary products or protocols in favor of a multi-vendor network environment based on DoD implementation of open system standards. With this approach, the NTBN will benefit from the wide range of new security and communications technologies which will emerge as both industry and Government continue their migration toward open system standards.

The recommended MLS approach for the NTBN is Architecture 1. It can be implemented at selected NTBN nodes on a prototype basis without requiring changes to the existing NTBN communications architecture based on multiple T1 circuits between nodes. Selection of Architecture 2 for near-term implementation would limit inter-node communications to 64 Kpbs, the throughput of a BFE device. Selection of Architecture 1 for a prototype system does not preclude eventual migration to an Architecture 3 packet switched MLS environment.

	ALTERNATIVE ARCHITECTURES		
EVALUATION CRITERIA	**1. Commercial MLS LANS connected by routers to existing comm. network**	**2. Single-level LANS connected to packet switched network by BLACKER/CANEWARE**	**3. Hybrid Combination of Architecture 1 and 2 features (MLS LANs, BFE/CFE, etc.)**
<u>Security</u> • Encryption • NCSC Evaluations	• MLS implemented at LAN device level • Encryption provided by KGs on comm. net. • A1 and B2 LANs have completed evaluations	• MLS implemented at WAN node level • Encryption provided by BFE/CFE • BLACKER meets A1 • CANEWARE meets B2	• MLS implemented at LAN device and/or WAN node level • Combines security features of Architectures 1 & 2
<u>Communications</u> • Compliance with Standards • Throughput	• B2 LAN based on Ethernet/TCP/IP; A1 on proprietary protocol • Uses high speed (e.g.T1) point-to-point comm.	• BFE/CFE comply with X.25, TCP/IP protocols • BFE limited to 64 Kbps • CFE (when available) will support T1	• Combines communications features of Architectures 1 & 2
<u>Availability of Key Products</u>	• MLS LANS now available from Verdix (B2), Boeing (A1) & Unisys	• BLACKER is currently available; CANEWARE available in 1 to 2 years	• Combines availability features of Architectures 1 & 2
<u>Acquistion Cost</u> (excluding labor for engineering and installation)	• Approximately $1M for interconnection of 200 workstations at multiple sites	• Approximately $1.6M for 100 BFEs and 20 packet switches at multiple sites	• Highly dependent on how Architecture 1 & 2 features are combined

Figure VI-3. Comparison of Alternative MLS Architectures

Examples of these alternative architectures, using currently available network security components, are provided in Appendix A.

3. Selected Architecture Specification

a. Overview

An MLS network will provide user support on the NTB at costs which are much lower than those incurred using multiple, single level networks.

MLS networks provide a means to share a physical transmission medium among several classification levels. The MLS network performs a separation of different classification levels so that access control is enforced based on user clearance and data classification. It is imperative that the MLS network operate correctly such that separation of classes is always maintained. Assurance of operational correctness is required to mitigate the risk of security compromise.

The MLS network architecture is best specified in three functional areas. The local area network (LAN), internet, and wide area network (WAN) backbone components will be specified in the following sections, and are illustrated in summary format in Figure VI-4.

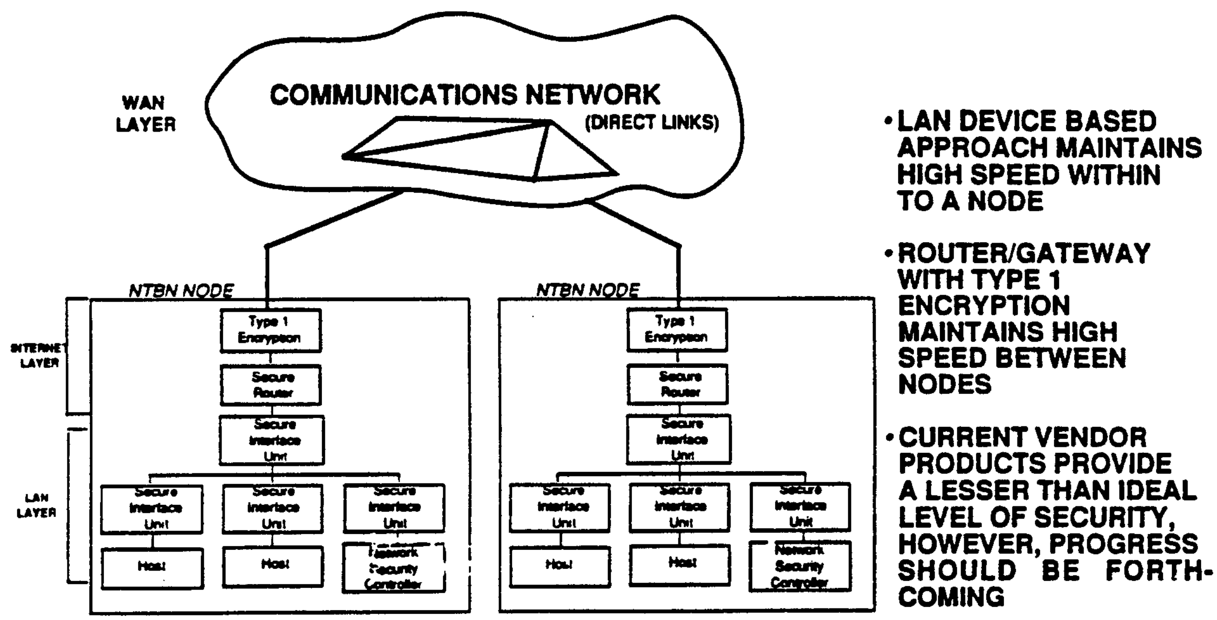


Figure VI-4. MLS-LAN Orientation for Architecture 1

b. Local Area Network

The local area network (LAN) component shall provide assured mandatory and discretionary access control mechanisms to provide separation of classification levels and need-to-know. The LAN shall be DoD standard protocol suite compliant - TCP/IP currently, GOSIP in the future. It shall securely interoperate with the Internet and WAN Backbone Layers.

The LAN layer will be able to support both single level and multilevel attached computers. Single level computers shall be treated at a security level commensurate with the clearance level of the users of the system. The security level of the system shall be set by a Network System Security Officer (NSO) in an assured manner.

MLS computers shall have a classification range (max-min) specified by the Network NSO. All data transmitted on the network shall be labeled according the classification set by the NSO. All received data shall be checked for label correctness and only that data which has been labeled consistent with the level of the computer shall be received by the computer.

c. Internet

The LAN shall be interoperable, in a secure manner, with wide area networks (see WAN Backbone below). The Internet shall provide this interoperability by using routers/gateways to provide assured relay of data with assured label integrity. The router/gateway must accept a labeled network packet and relay that packet without making any changes to the data classification label. The Internet layer must be interoperable with current and future DoD protocol suites.

d. Wide Area Network Backbone

The Wide Area Network (WAN) Backbone shall provide assured mandatory and discretionary access control mechanisms to provide separation of classification levels and need-to-know. The WAN Backbone shall be DoD standard protocol suite compliant - TCP/IP currently, GOSIP in the future. It shall securely interoperate with the LAN and Internet components.

The WAN Backbone will be able to support both single level and multilevel attached computers. Single level computers shall be treated at a security level commensurate with the clearance level of the users of the system. The security level of the system shall be set by the NSO in an assured manner.

MLS computers shall have a classification range specified by the NSO. All data transmitted on the network shall be labeled according to the classification set by the NSO. All received data shall be checked for label correctness and only that data which has been labeled consistent with the level of the computer shall be received by the computer.

The WAN Backbone shall provide formal assurance proofs of the correct operation of all network security mechanisms.

VII. SYSTEM IMPLEMENTATION PROGRAM OVERVIEW

A. Phasing

The proposed three-part phasing of the MLS implementation is shown in Figure VII-1. The near-term (FY 91-93) and mid-term (FY93-95) phases provide for NTBN upgrading to an initial MLS capability. The long-term (FY95-99) phase involves incorporation of features for increasing MLS security assurance.

In comparing NTBN security goals and requirements to predicted technological advances, great care was taken to be realistic and objective. It is anticipated that the National Security Agency (NSA) will continue to place high priority on evaluating an even greater number of Computer Security (COMPUSEC) products at even higher levels of COMPUSEC trust in the years ahead. Increased assurance of secure operation is gained as products evaluated at higher

levels of COMPUSEC trust are incorporated. The increased assurance is indicated by upgrading from a B3 level of trust to an A1 level. (B3 and A1 are the technical terms used by the NSA and DoD to indicate the degree of trust (i.e. assurance of secure operation) that a computer system has achieved.) A system accredited at the A1 level incorporates security products and safeguards that offer significantly higher levels of trust than those needed for B3 accreditation. The NTBN must have the highest possible degree of trust to minimize the risk of security compromise. Therefore, a phased approach is recommended to achieve higher levels of assurance as the technology becomes available.

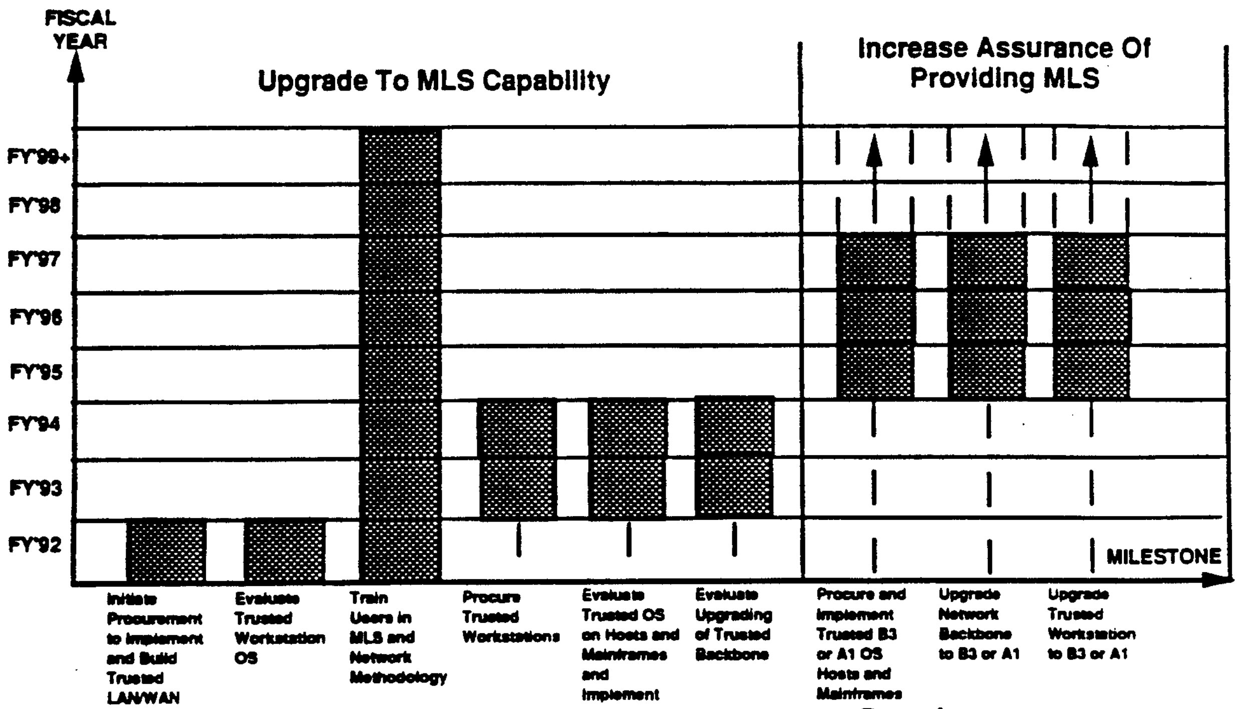


Figure VII-1. System Implementation Program Overview

1. <u>Near-Term (FY-91-93)</u>

Near-term goals of the trusted MLS implementation are to:

(1) Prepare design documentation and implementation plans for a first-generation MLS LAN;

(2) Implement/build a trusted LAN/WAN;

(3) Evaluate trusted workstations and trusted operating systems for all hosts and mainframes;

(4) Train all users in use of trusted LAN/WAN resources.

In order to begin the implementation of a trusted MLS LAN in FY-92 there must first be a detailed LAN/WAN design leading to specific hardware and software specifications. This design should be developed by a follow-on group to the Tiger Team, which would subsequently make recommendations for hardware and software procurements. Installation, implementation, and testing of the trusted LAN/WAN should be initiated in FY-92.

A working group should be formed in FY-92 to evaluate trusted workstation technology. A trusted workstation should be chosen (perhaps more than one type/vendor) for use on the NTBN. The workstation will become the mainstay of, and interface

with the trusted LAN; thus it must be evaluated with regard to growth, evolution, and interoperability. A B-rated technology such as Compartmented Mode Workstation (CMW) should be the minimum level of trust accepted for a workstation to access MLS LAN network.

All users of the NTBN must be trained to use the new MLS technologies as they are implemented. Such training should include some basics on NTBN high-level design and topology and should also include LAN/WAN operational procedures and computer security practices. This training is important to acclimate the users to the MLS technologies.

2. Mid-Term: (FY-93-95):

During the mid-term phase of MLS implementation, the following tasks should be accomplished:

(1) Procure and implement trusted workstations;

(2) Evaluate and procure trusted operating systems for use on all hosts and mainframes;

(3) Train personnel in the use of trusted workstations and trusted LAN/WAN resources;

(4) Evaluate the possibility of upgrading the trusted network backbone (as technology allows).

During FY-93, procurement of the trusted workstations should begin, and by FY-94, their implementation should be fully completed. The implementation of trusted workstations should greatly increase the productivity of the NTBN users by allowing ease of access to a multiple array of resources via the MLS network from a single MLS workstation.

The evaluation and procurement of trusted operating systems for use on all hosts and mainframes should be initiated in FY-93 and completed by FY-94. Trust at the B-level should be the goal for initial operating system implementation on the NTBN. This level of trust for the operating systems is consistent with implementation of B-level LAN/WAN technology and B-level workstations with mandatory access control. Where this goal is not feasible for initial operating system implementation, it should continue to be a longer-term goal to be achieved as technology advances. This goal for B-level trust in operating systems should be an on-going endeavor, since the intent of the NTBN is to operate at the highest level of trust technologically possible.

User training of the trusted workstations should be initiated concurrently with their implementation. This training should include all facets of workstation use including interface to the trusted LAN/WAN. Operational procedures and computer security practices should also be included.

During the mid-term phase of MLS implementation, the possibility of upgrading the trusted network backbone (LAN) to a higher degree of trust should be investigated. If such an upgrade is determined to be both feasible and necessary, the appropriate budgetary programming should be made.

3. Long-Term (FY-95-99):

Over the long-term, the MLS implementation involves the following tasks:

(1) Procure and implement trusted B3 or A1 operating systems for hosts and mainframes;

(2) Upgrade trusted network backbone to B3 or A1;

(3) Upgrade trusted workstations to B3 or A1.

The long-term goal for the MLS implementation is to achieve the highest degree of trust technologically possible within program budgetary constraints. Procurement of trusted operating systems at the B1 or B2 level for hosts and mainframes should be accomplished in FY-93 (during the mid-term phase). During FY-95, these should be upgraded to the B3 degree of trust. The ultimate goal for the NTBN should be operation at the A1 security level. This will require implementation of an A1 certified network backbone, as well as A1 trusted operating systems for all hosts and mainframes. Achievement of this level of trust will depend on the level of the available technology during this period, as well as the cost of implementing the new technology. By FY-95 or FY-96 the operating systems available for the trusted workstations may include B3 or even A1 certified systems as well. These systems should be incorporated as they become available, within budgetary limitations.

B. Functional Responsibilities

In order for the phased implementation of the MLS (secure NTBN) to be successful, the functions required to achieve that implementation must be clearly defined. The functions will be the responsibility of the organizations which use and maintain the NTBN. Those organizations are SDIO, NTBJPO, the NTF, the user organizations at the NTBN nodes, and the Executing Agents (EAs). The functions relative to this effort include, but are not limited to, the following:

(1) Obtain top-level program funding for installation, operations and maintenance, and systems engineering of an operationally effective NTB with the proper security safeguards.

(2) Ensure use of the NTB as a common testing resource by coordinating NTB resources with related SDI program requirements.

(3) Obtain a common ground among different security agencies (DoD, DOE, DIS), so a single system can be accredited for use by members of all agencies.

(4) Establish NTBN interface requirements for all node resources connected to the NTBN.

(5) Engineer, install, operate, and maintain the NTBN (connect all nodes to the NTBN backbone).

(6) Develop and maintain an NTBN standard interface for connecting NTB resources to the NTBN.

(7) Identify the node resources to be made available for use by the NTB.

(8) Provide guidance/assistance to all nodes on ways to secure resources which interface with the NTBN.

(9) Maintain the resources (hardware, software, personnel) for the centralized management, control, and evaluation of the NTBN.

(10) Include NTBN interface standards in all contracts which require connectivity to NTB resources.

(11) Provide necessary testing and documentation to achieve and maintain accreditation of the NTBN.

C. Support Elements

Along with the implementation of hardware and software components to make an MLS network, a support structure must be developed to achieve/evolve to an MLS operational mode of the NTBN. Support elements include operations and maintenance, training, testing, and system engineering of the NTBN. Even though element support requirements will affect all nodes to some extent (network management and security management) it is expected that the infrastructure for these elements would be provided by the NTB and located at the NTF. Manpower, hardware/software resources, and security clearances must be considered for the following task:

(1) O/M - Install the selected components of the MLS network.

Develop/maintain the standard interface kits.

Install upgrades/improvements of network products as they become available.

Provide network hardware/software configuration management.

Provide operational network (reconfiguration) management.

Provide network security management.

(2) Training - Provide training to support the operations and maintenance of network components.

Provide training on the use of tools and the NTBN topology in support of network/security management.

Provide training to the users of the NTB network. The goal is to keep this training requirement to a minimum by providing a network which is transparent to the user.

(3) Testing - Test the network for compliance in terms of usability, throughput, growth, etc. This is a recurring requirement as the network is expanded and/or upgraded.

Test the network to ensure proper use/configuration of the security components of the network. This is a continuing requirement to provide additional assurance of the MLS capabilities of the network.

(4) System Engineering - Develop the NTBN standard interface requirements using national networking/communications standards.

Develop the NTBN detailed designs in support of all implementation phases.

Evaluate new and improved hardware/software products to provide increased assurance/performance of network and incorporate selected components into the NTBN design as they become available.

Provide engineering support to the security accreditation process.

Provide engineering support in the development of node enhancements to improve the NTBN MLS capabilities.

Provide the follow-on engineering support to ensure compliance of the Tiger Team recommendations.

D. Follow-on Efforts

A working group has been formed to complete systems engineering work which will provide the basis for implementing a first-generation MLS network. This working group will prepare an MLS Network Requirements Document describing the minimum capabilities needed in a first generation MLS network. The document will also list security and performance objectives for future upgrades to the first-generation network. The working group will also prepare an MLS Network Program Plan which includes schedule goals, estimated costs, and organizational responsibilities for network implementation.

VIII. CONCLUSIONS

This report recommends a multilevel secure architecture to meet the SDI community's need for a data transfer network which can restrict user access to data based on a range of security considerations including clearance level, need-to-know, citizenship status, and corporate affiliation. The recommendation was driven by three key factors. First, a cost analysis showed that it will be prohibitively expensive over the long term to duplicate communications and processing systems for each set of NTBN users who are not allowed access to the existing set of single-level networks. Second, the proliferation of single-level networks will adversely affect operation by forcing some users to rely on two or more networks to perform a task which could be performed more efficiently on a single, integrated network. Finally, a technology survey showed that components of a first-generation MLS network are now commercially available as a result of recent industry and Government-sponsored product development and evaluation efforts.

The recommended NTBN architecture meets user requirements identified in this report and provides a basis for modular and flexible growth to accommodate new requirements and technologies as they are identified. The selected architecture includes:

(1) A LAN component which conforms to the DoD standard protocol suite and supports secure, high-speed communications with single or multilevel hosts.

(2) An Internet component consisting of secure routers/gateways, which support the DoD protocol suite and secure, high-speed communications with single or multilevel hosts.

(3) A WAN backbone which supports the DoD protocol suite and secure interconnection of NTBN nodes through the LAN and Internet components.

The Tiger Team's recommendations for implementing the recommended architecture include:

(1) Completing the systems engineering, design and planning activities required to gain management approval for procuring MLS networking components.

(2) Installing a first-generation MLS network in FY-92 and performing proof-of-concept testing of key elements of the recommended architecture and detailed network design.

(3) Establishing DAA MOAs to encompass responsibilities and security policies for protection of classified information on AISs and the NTBN.

(4) Establishing an NTBN configuration control board.

(5) Beginning a follow-on effort to define an approach for providing trusted workstations and hosts.

APPENDIX A

APPENDIX A

Architecture Evaluation

I. INTRODUCTION

As described in the body of this report, there are two major architectural network designs that could be employed to provide network security for the National Test Bed: multiple, single level networks or a single, multilevel secure (MLS) network. This appendix provides implementation details and cost estimates for these network designs.

A. Multiple, Single Level Networks

The specific details of implementing the multiple, single level networks architecture are well known to the NTB community because this is the current NTB network architecture. A number of additional networks and computers will be required if this architecture is to continue to support all of the classifications and compartments needed for the future NTBN.

This architecture would make use of separate, isolated facilities to support users at specific clearance levels. Each of the separate networks would need its own communications system to provide interconnectivity between NTBN sites. Users with specific clearance levels will be located at various NTBN sites and will need access to various types of computing resources. Communications security (COMSEC) equipment will be necessary to ensure the confidentiality of data transmitted between sites.

The majority of security mechanisms and features employed in this architecture are related to physical security rather than system security. Users would have physical access to terminals, workstations, and computers that are connected to the network that contains data at the user's clearance level. Therefore, for example, users who have a secret clearance would only have physical access to the secret network and its facilities. They would not be allowed access to any other network's facilities. Physical access control to the facility can be accomplished in several manners such as by having guards checking facility access lists, by badge readers connected to facility access computers that check access control lists, or biometric checking equipment (retina scan, fingerprint, voice print) connected to facility access computers.

Security policy typically allows data to flow up from a lower classification level to a higher classification level. In this manner, a Secret cleared user has the ability to read all the data at his level and below without a security compromise. However, with multiple, single level networks that are totally isolated, the user will not have the ability to read any data except at the specified clearance level. In order for data to flow up, one-way gateways could be used to allow the interconnection of the single level networks. The one-way gateways would provide high assurance that data will flow only in one direction, from low to high and that there will be no data flow from high to low. In effect, the gateway acts as a diode, allowing flow in one direction only. There are several candidate systems implemented with high assurance security reference monitors that could be used to build such a gateway (HFSI XTS-200, Gemini, Loral MLS-100). Although several of the systems are NCSC evaluated (or soon to be), the gateway application would have to be separately evaluated and shown to provide the necessary assurances with respect to data flow. It would then be up to the Designated Approving Authority to decide whether to allow such interconnection among the various single level networks.

The costs associated with multiple, single level networks can be determined by the number of networks needed, the computing resources, the physical security controls, and the administration and operations personnel that need to be duplicated among those networks. As previously described in Section VI, if users on each separate network require simultaneous access to a CRAY, then a CRAY would have to be procured for each network at the current price of a CRAY. In addition, operators for each CRAY, for each network control center, and for all of the other computing resources would be required. Table A-1 provides cost estimates for purchasing and operating six new Cray computer systems as part of separate, single-level networks.

Table A-1. Cost Estimate For Six Cray Systems As Part Of Multiple Single-Level Networks

Cost Item	Nonrecurring Cost	Recurring Cost (Annual)
Computer Systems HW/SW	$110 M	
Communications Systems	$ 3.3 M	
ADPA Operational Support		$ 2.6 M
Vendor Maintenance Support		$ 5.4 M
External Circuits	———	$ 8.8 M
TOTAL	$113.3 M	$16.8 M/YR.

B. Single, Multilevel Secure Network

A single multilevel secure network is a major departure from the existing NTB architecture. The MLS network will require the use of network components that do not degrade current network performance, are reliable, maintainable, and provide assurance of correct operation with respect to security enforcement mechanisms. The assured operation of security mechanisms is the basis upon which the network is trusted to provide data separation, based on data classification, on the network. The MLS network will use components which have been designed and developed in compliance with NCSC guidelines. The types of components under consideration here are network security interface devices, network security front-end devices, routers/gateways, bridges, packet switching equipment, and COMSEC devices.

In the near-term, a single, multilevel secure network can be built using existing, commercially available network security products. These current products implement computer security features and mechanisms, but are lacking in the area of high assurance of correct operation. An example MLS network of this type is the Verdix Secure Local Area Network (VSLAN) which has been evaluated by the NCSC and rated at the B2 (MDIA) level. This rating indicates that the VSLAN provides mandatory and discretionary access control (MAC/DAC) as well as identification, authentication and auditing. However, at the B2 level, there are no requirements for design or implementation assurance of correctness of operation. Without such assurance, the number of classification levels that can simultaneously be supported on the same network is limited (ref Yellow Book). These limitations will be discussed further in the following paragraphs.

For the long-term, the NTB should utilize MLS components that provide high assurance of correct security operation. These high assurance products provide the same base security functionality as do their low assurance counterparts, but provide the additional assurance that those security functions/mechanisms operate as they were designed, with no additional functional or side effects that could compromise system security.

The VSLAN is an IEEE 802.3 (Ethernet) LAN. The evaluated components of the VSLAN are the Verdix Network Security Device (VNSD) and the Verdix Network Security Controller (VNSC) as shown in Figure A-1. The VNSC is the security officer operations center that provides the NSO with the tools for initializing, administering, and controlling the network. The VNSDs are hardware boards that are installed in each of the network computers and are controlled by the VNSC. Verdix currently produces boards for many computer bus configurations (e.g., QBus, VME, Multibus, PC-AT) and has several more under development.

The VNSDs are MLS trusted devices that operate with a security kernel running on an Intel 286 processor on the VNSD board. The VNSDs are defined by the VNSC to be operating at a specific security level (when installed in a single level computer) or at a range of levels (when installed in a multilevel computer). Source and destination computer systems are identified and authenticated by the use of DES encryption and a datakey inserted into a receptacle connected to the VNSD board.

A VSLAN NSC can control 128 computers on a secure network segment. In order to provide connectivity for more computers, as well as to computers at remote sites (e.g., NTF, SDC, GE) a router/gateway device is needed. The Verdix Secure IP Router (VSIP) is a secure router that is able to securely interconnect two VSLANs or can interconnect a VSLAN and a single level Ethernet. This device can be used to interconnect networks in a local facility such as the NTF or between facilities using COMSEC devices to provide confidentiality on the transmission medium.

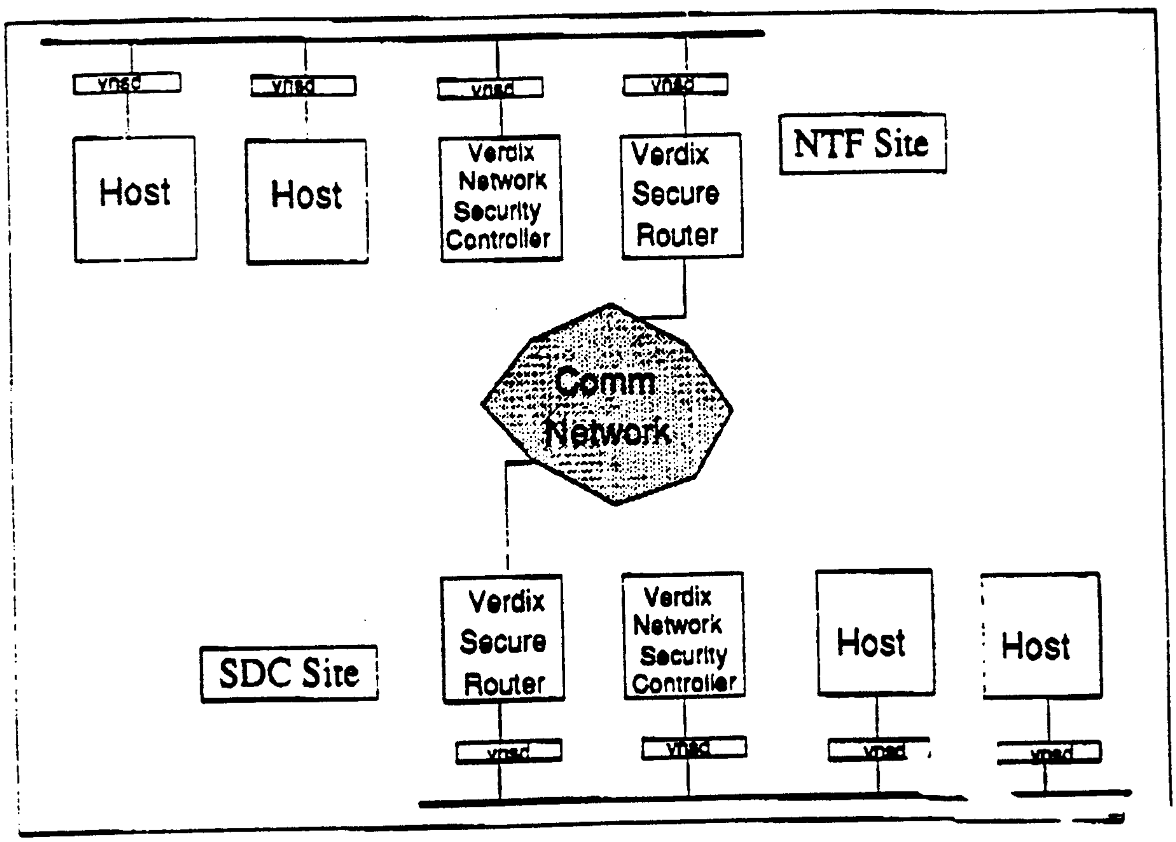


Figure A-1. Single MLS Network Using Verdix

Using a VSLAN architecture, several classification levels can be combined onto a single MLS network. Because the VSLAN is rated B2, not all the required classification levels can be combined onto the same network. This is a result of the risks that are involved in using network components that do not provide high levels of assurance of operation. *The Guidance For Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* (CSC-STD-003-85, also called the Yellow Book) provides guidance in deciding how many levels of classification can be combined on an MLS system based on its evaluation rating. Using Yellow Book guidance, all of the Secret level networks and the Top Secret networks could be combined using a B2 network, but Unclassified users would have to be kept separate or connected via a special, high assurance gateway. Only with a system that provides higher assurance of correctness could more levels be simultaneously connected. However, this architecture does succeed in eliminating most of the replicated networks.

VSLAN implementation costs are variable. Each PC or workstation could have a VNSD board inserted for attachment to the network (at a cost of $4250 per board in single quantities with volume discounts available), or communities or PCs and workstations could be connected as a single level community of interest using a router onto the secure network backbone. Each mainframe system would have a VNSD board (if available for the specific processor) or could have a VNSD in a front-end system (e.g., a SUN front-ending a CRAY). The Verdix Secure IP Router costs $12,000 and a Verdix Network Security Controller costs $17,500. The total implementation cost would be determined by the final network topology which would result in a determination of how many copies of each device would be required. As an example, if there were 200 computers that were to be directly connected to the VSLAN (e.g., VNSD boards directly inserted into their backplanes) the cost would be no greater than $850,000 (actual cost would be lower based on volume discounts). In addition at least two VNSCs would be needed since each VNSC controls up to 128 attached computers. Therefore, there is an additional cost of $35,000. There would also be a need for several VSIP (routers) devices (approximately 10), resulting in additional cost of $120,000. Therefore, for these strawman numbers, a total installation of VSLAN hardware products would cost approximately $1.05 million. There would be additional charges for communications lines interconnecting the NTB sites. This can be compared to the cost of replicating a network many times (including the $90 million for replicated CRAYs) and it appears to be a very good manner in which to proceed to save large amounts of money.

An alternative MLS architecture can utilize the Government-developed BLACKER family of network security equipment as shown in Figure A-2. BLACKER products are currently available, and products from the related CANEWARE program will be available in FY1992. BLACKER has been evaluated by the NCSC and has been given an A1 rating. CANEWARE will be evaluated as a B2 device. In addition, BLACKER has been evaluated from a COMSEC perspective and is endorsed as a high grade, Type 1 cryptolographic equipment. BLACKER has been certified for use by the Defense Data Network (DDN) to combine its three, separate classified DISNET networks (SECRET, TS, and TS/SCI) into one network sharing a common backbone. Both BLACKER and CANEWARE were designed to operate over packet switched networks and interface to Packet Switching Nodes (PSN). BLACKER interfaces to PSNs using the DDN-X.25 standard and CANEWARE uses the DDN-X.25 or CCITT-X.25 standards. BLACKER will run at 64 KBits/second and CANEWARE will run up to T1 interface speeds (1.544 Mbits/second).

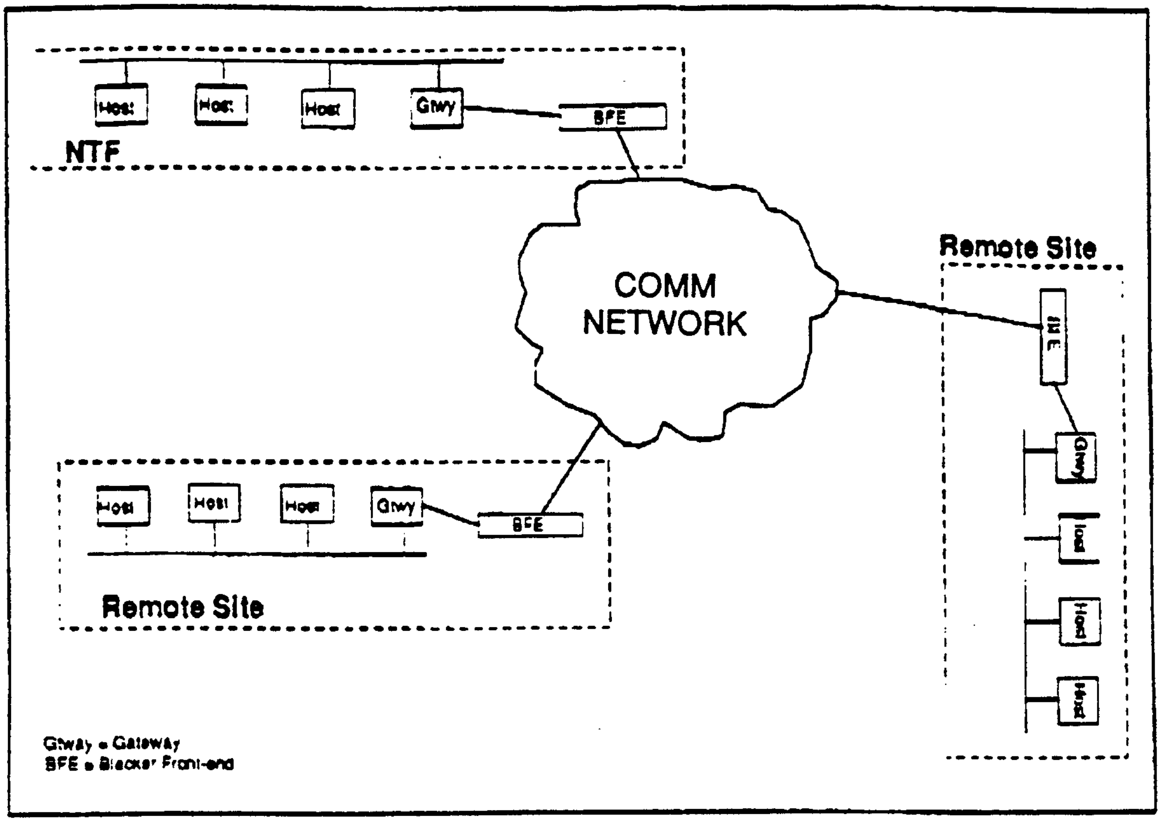


Figure A-2. Single MLS Network Using BLACKER

In a BLACKER architecture, the network interface of a host or community of hosts would be a BLACKER Front End (BFE) device. The BLACKER would provide access control, source-to destination identification and authentication, and data confidentiality. Because BLACKER is rated A1, there is less risk in combining different classification levels than with a B2 system. The A1 rating signifies that the design was formally specified and that rigorous proofs have been performed to provide evidence that the system operates correctly. Unclassified through Top Secret is still not advised (based on the Yellow Book), but A1 does allow confidential users to be added to the network with Top Secret or even multiple Top Secret compartments. CANEWARE, when it is available, will provide higher line speeds than BLACKER.

To implement an MLS network using BLACKER (or CANEWARE) equipment, a packet switching network must first be procured and installed. The packet switching network could be a technology copy of the DDN using Bolt, Beranek, and Newmann (BBN) DDN Packet Switching Nodes. Alternatively, the DDN DISNET could be used as the interconnection medium between NTB sites. Hosts would be connected to BLACKERs which in turn would connect to PSNs. BLACKER makes use of an Access Control Center to make mandatory (classification) and discretionary (need-to-know) access control decisions. A Key Distribution Center is used to distribute cryptolographic keys based on a source/destination/classification connection basis.

BLACKER devices cost approximately $10,000 each, not including installation. To effectively use BLACKER, the network topography should make extensive use of single or multilevel level local area networks that would be gatewayed through a BLACKER onto the MLS network backbone. In this way, the number of BLACKERs required would be minimized without

effecting the overall security of the MLS network. If the NTB were to need 100 BLACKERs, the cost would be approximately $1 million. In addition, packet switching equipment would be needed at each of the sites. A BBN C/30 packet switch costs approximately $30,000. A 20-switch network would cost $600,000. In addition there would be charges for network usage (e.g., DISNET charges of $60,000 per year or private line charges if DISNET were not used to interconnect the sites).

Another alternative architecture, as already alluded to in the previous paragraph, is the combination of secure LAN and BLACKER/CANEWARE products as shown in Figure A-3. The LAN products are typified by providing higher throughput speeds than BLACKER/CANEWARE. In this manner, the local users at a specific site can enjoy the higher speeds afforded by using Ethernet or fiber cable plants and only use the lower speed interconnections when going between sites. A current problem in using this architecture is the inability of the current generation Verdix devices to allow a security label to be exported to a non-Verdix network. A Verdix Secure IP Router with a non-VSLAN interface (Ethernet) would not export a label. The LAN would treat the Ethernet as a single level network. This would be true even if a multilevel BLACKER were on the other side of the Ethernet. A secure router would have to be designed and built to provide this MLS connectivity across networks. The VSIP, Gemini, Loral, or HFSI equipment could be used as secure gateway platforms to perform this function.

NTB NETWORK Security Architecture

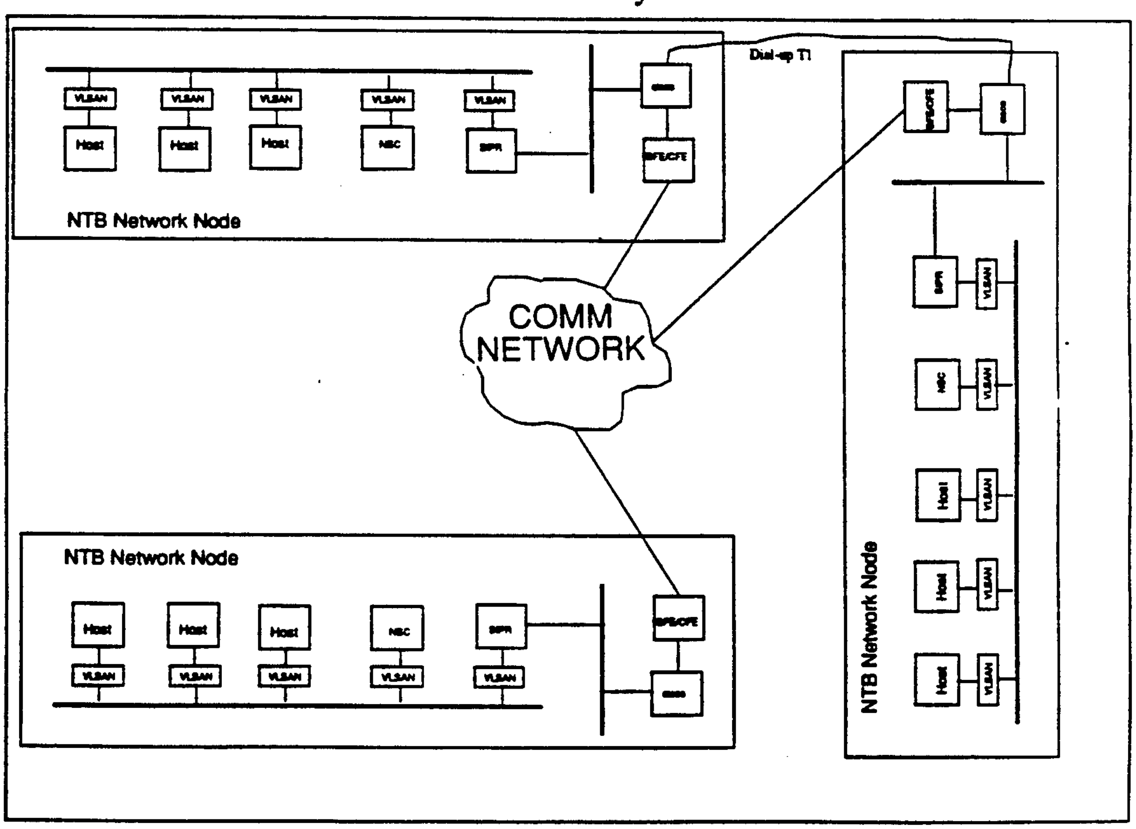


Figure A-3. Single MLS Network Using BLACKER and VERDIX

APPENDIX B

Guidance and Requirements Document

GUIDANCE AND REQUIREMENTS

FOR A

MULTILEVEL SECURE

NETWORK

TO SUPPORT

THE STRATEGIC DEFENSE INITIATIVE

APRIL 1992

EXECUTIVE SUMMARY

A. INTRODUCTION

The "NTB Network Security and Communications Report" completed by the National Test Bed (NTB) Security and Communications Architecture Working Group (SCAWG - also called the "Tiger Team") provided the definition of a system architecture, operational concept, and system implementation approach to provide secure and integrated information transfer and shared computing capabilities to support the NTB mission. These capabilities will be achieved by evolution of the existing National Test Bed Network (NTBN) and NTBN nodes.

The Tiger Team began its work in March 1991 and met regularly for five months. Initial Tiger Team efforts focused on identifying system requirements and investigating available technologies in the areas of security, automated information systems (AIS) interfaces, communications, and control. The Tiger Team evaluated alternative architectures, operational concepts, and implementation approaches based on their projected cost and responsiveness to system requirements.

The Tiger Team report recommended a multilevel secure architecture to meet the SDI community's need for a data transfer network which can restrict user access to data based on a range of security considerations including clearance level, need-to-know, citizenship status, and corporate affiliation. The recommendation was driven by three key factors. First, a cost analysis showed that it will be prohibitively expensive over the long term to duplicate communications and processing systems for each set of NTB users who are not allowed access to the existing set of single-level networks. Second, the proliferation of single-level networks will adversely affect operations by forcing some users to rely on two or more networks to perform a task which could more efficiently be performed on a single, integrated network. Finally, a technology survey showed that components of a first-generation Multilevel Secure (MLS) network are now commercially available as a result of recent industry and Government-sponsored product development and evaluation efforts.

This report builds upon the Tiger Team report and extends the architecture to include both MLS communications and computing. It describes an MLS Network security architecture and provides the guidance, requirements, and recommendations necessary to commence the design, development, and implementation of an MLS Network to support the communications and computing needs of the SDI community. It includes a phased implementation of secure interface units starting at the NTF LAN, progressing to the NTBN, and finally to implementation of secure operating systems and applications on selected mainframes and workstations. It includes the use of prototyping during the near term to ensure the success of later phases.

B. SECURITY GOALS

The need for security in the NTB environment is dictated by the sensitivity of information and the internal and external threat of compromise of that information. Security as such is an enabling technology which provides a wide range of users access to shared computer and communication resources which process information at multiple levels of classification. The challenge in providing the needed security is defined by the environment within which the NTB mission must be performed. The key elements of the mission environment include:

(1) Dispersed geography with many AIS platforms and many requirements to communicate;

(2) A wide range of users from Government, industry, and various U.S. Allies; and

(3) A wide range of security classification levels required.

The fundamental security goal is therefore to support the simultaneous accessing and processing of Unclassified, Unclassified Sensitive, and Classified SDI data by a wide range of users with different security clearances and authorizations. The specific security requirements for access restrictions, data integrity, user identification and accountability, and system integrity must be resolved to successfully achieve this goal. The MLS Network will be achieved through a phased implementation consisting initially of currently available trusted components for the near term MLS NTF LAN (FY92-93), with a planned migration path through the mid term MLS NTBN (FY93-95), to the long term MLS NTBN and NTBN nodes (FY96-99). Current and projected security products and technologies will be incorporated to fully meet all security requirements and objectives.

C. SUMMARY OF REQUIREMENTS

Access to data must be restricted to only those users who are appropriately authorized for that data. Authorizations shall be based on a user's security clearance, need-to-know, and restrictions resulting from organizational conflicts of interest and a user's citizenship. To meet the projected user requirements and to enhance the current capabilities, the MLS Network, and in particular the NTF LAN and the NTBN must support an MLS mode of operation. The MLS requirement is directly driven by the SDI requirement to "provide a common test environment for the design of GPALS", and by the wide participation of Government, academic, industry, and allied nation organizations.

The requirement for flexibility is derived from both the changing mission environment and the evolution of test phases as cited by the SDIO user community. The mission environment is altered by the redirection of SDIO toward theater and tactical considerations which in turn may alter the required geographic dispersion of supporting NTB resources. The evolution of test phases indicate that many of the programs in SDIO are still in the early stages of development, and as development progresses test complexity and scope will expand. New sites will be added and must be accommodated.

The requirement for modularity follows the derivation of the requirement for flexibility, and the need to support a shared resource user community. With a dynamic user community accessing a shared resource, a common set of mechanisms for providing that access is essential for responsiveness. A modular approach allows the network to easily adapt to varying data capacity and security requirements, making resources available as they are needed. Thus modularity is a critical characteristic that must be incorporated in a responsive security architecture.

The need for standardization (and conformance to a guiding set of standards) derives from the dynamic nature of the NTB user community and from public law, DoD policy, and federal policy. Standardization of security mechanisms, communications mechanisms, and operational procedures will be essential to maintaining a responsive MLS Network over its life cycle. The selection of a guiding set of standards for the architecture is driven by this need for supportability and maintainability; however, it is also recognized that standards in communications and security are still evolving and thus the architecture must be flexible enough to evolve with those standards.

D. SUMMARY OF RESULTS

To achieve the security goal, an MLS Network that will preserve the integrity of sensitivity labels and use those labels to enforce mandatory access controls based on the differing clearance levels and authorizations of individual NTB users must be developed and implemented in accordance with the computer security requirements specified in DOD 5200.28-STD, DOD Trusted Computer System Evaluation Criteria. Based on the determination and application of the Risk Index to the MLS Network security components in accordance with the guidance provided in CSC-STD-003-85, "Application of Computer Security Requirements In Specific Environments", for "closed" security environments, the near term (FY92-93) requires a class B2 level of assurance as a minimum, the mid term (FY93-95) requires a class B3 level of assurance as a minimum, and the long term (FY96-99) requires a class A1 level of assurance as a minimum. The Risk Index is an indication of the disparity between the minimum clearance or authorization of users and the maximum sensitivity (e.g., classification and categories) of data processed by the MLS Network.

A number of factors were considered in designing the security architecture to meet the required levels of assurance. First and foremost, the security components must comply with all specified security requirements. Second, to ensure affordability, the security components must be National Security Agency (NSA) evaluated/certifiable commercial-off-the-shelf (COTS) trusted security products to the maximum extent possible. Finally, a cost effective and well planned migration path must be provided to transition from the near term to the long term.

The security architecture addresses all these factors and related issues by initially providing a minimum of a B2 MLS NTF LAN in the near term. There are two distinct approaches for achieving the B3 mid term and A1 long term requirements. The first approach is the modular replacement of B2 evaluated components with NSA evaluated/certifiable B3/A1 components. The second and recommended approach is to select A1 evaluated/certifiable components for use starting in the near term. To facilitate either approach, the security architecture must be designed from the beginning to meet A1 requirements. This will be accomplished by developing the initial security assurance documents (philosophy of protection, and informal and formal security policy models) to meet A1 requirements, designing the security architecture based on the A1 security policy model, and modularly partitioning the design to facilitate the use of additional A1 products as they become available.

In addition to meeting all computer security requirements, Communications Security (COMSEC) and TEMPEST countermeasures will be implemented in accordance with SDIO Directive 5206, established regulations, directives and procedures. Likewise, physical and procedural security will be implemented in accordance with the appropriate guidelines.

E. CONCLUSIONS

To support the simultaneous access of information with different sensitivities by users with different clearances and need-to-know, and to prevent users from obtaining access to information for which they lack authorization, the MLS Network must enforce Mandatory Access Control (MAC) and Discretionary Access Control (DAC). The near term security operating mode will be MLS and will initially require a minimum of a B2 level of assurance to support users with a minimum clearance of Secret and to simultaneously process Unclassified and Classified (up to Secret with multiple categories) information. In the near term, the NTF LAN will operate in the MLS mode and will simultaneously support multiple communities of interest located at the NTF. A community of interest is a closed user group that permits users belonging to a group to

communicate with each other, but precludes communications with other users who are not members of the group.[1]

The mid term MLS NTBN security operating mode will also be MLS, but will require a minimum of a B3 level of assurance to support users with a minimum clearance of Secret and simultaneously process Unclassified and Classified (up to Top Secret with multiple categories) information. In the mid term, in addition to the MLS NTF LAN, the MLS NTBN will provide simultaneous support and access to NTF resources to users at the other NTBN nodes operating in different communities of interest. The remote NTBN nodes will still operate as single level communities of interest.

The long term MLS NTBN and NTBN nodes will require a minimum of an A1 level of assurance to support users with no clearance and simultaneously process both Unclassified and Classified (up to Top Secret with multiple categories) information. During the long term, the network will provide for MLS access to databases and computing resources and some of the NTBN nodes, other than the NTF, will operate in the MLS mode.

[1]NCSC-TG-005, Version 1, pg 264.

GUIDANCE AND REQUIREMENTS FOR A MULTILEVEL SECURE NETWORK TO SUPPORT THE STRATEGIC DEFENSE INITIATIVE

I. INTRODUCTION

This document, which is derived from the Tiger Team recommendations and conclusions, provides guidance and requirements for the next phase in the design, development, and implementation of an MLS Network. The architecture and implementation proposed extend the definition of a solution to the problems (high cost, restricted data exchange between communities of interest (COIs), and limited resource sharing) associated with the continued proliferation of dedicated mode networks, nodes, and AISs. The MLS Network will evolve from the existing system high NTBN and dedicated and system high NTBN nodes.

This document consists of seven sections and four attachments: Section I, Introduction, defines the scope and objectives of the document and provides background information on the Tiger Team report and its conclusions. Section II, Definitions, provides a set of basic working definitions used throughout the remainder of the document. These definitions establish the framework for the architecture by specifying the characteristics of an MLS Network and its security components. Section III, Need for MLS Communications and Computing Environment, provides an overview of the requirements. Section IV, Evolutionary Approach, describes the changes to be made as the NTBN and NTBN nodes evolve from the existing Secret/CW system high NTBN and dedicated and system high NTBN mode nodes to the MLS mode network. Section V, Requirements, contains the functional, performance, and security requirements for the near, mid, and long terms. Section VI, Security Architecture, identifies and describes the projected modes of operation of various components during the three phases, describes "risk index" and "open" and "closed" environments and their relationships, shows the computation and derivation of the level of trust requirements, and contains figures showing allowable data transfers and COI segregation. Section VII, Preliminary Implementation Architectures, describes the use of secure interface units to segregate data based upon COI and contains figures which show equipment configurations that produce an MLS NTF LAN, NTBN, and AISs in the near, mid, and long terms, respectively. Attachment I, Boeing Secure Network Server (SNS) and Network Manager (NM) Capabilities, describes the SNS and NM. Attachment II, Security Engineering Process, describes the documentation, engineering, and testing that will be required to evolve the NTBN and NTBN nodes to MLS mode. Attachment III, MLS Network Prototyping Plan, provides the schedules, estimated resources and prototyping methodology to be used in the development of an initial prototype and the phased enhancements to the initial prototype necessary to support the implementation and migration from the near term to the long term environments. Attachment IV, NTB Security Strategy Working Group Report, addresses the development of the NTBN Security Architecture.

A. Scope and Objectives

This document provides guidance and identifies the requirements for implementing a first generation MLS Network in the near term that provides support to NTB users with a minimum of a Secret clearance simultaneously operating in multiple COIs. In addition, it provides guidance and requirements for the evolution of the MLS NTBN and NTBN nodes in the mid and long term timeframes. The long term objective is to provide the capability for simultaneous connectivity for uncleared and cleared users with data sensitivity levels ranging from Unclassified to Top Secret with multiple categories.

B. Background

The NTB Security and Communications Architecture Working Group (SCAWG - also called the "Tiger Team") report provides a definition of an architecture, operational concept, and implementation approach to provide secure and integrated information transfer and shared

computing capabilities to support the NTB mission. The Tiger Team report recommended that the MLS Network evolve from the existing system high NTBN and dedicated and system high mode NTBN nodes.

The Tiger Team began its work in March 1991 and met regularly for five months. Initial Tiger Team efforts focused on identifying system level requirements and investigating available technologies in the areas of security, AIS interfaces, communications, and control. The Tiger Team evaluated alternative architectures, operational concepts, and implementation approaches based on their projected cost and responsiveness to system level requirements. The Tiger Team's recommendations were approved by representatives of the Government organizations and support contractors. Government representatives included SDIO/POI, SDIO/SIS, SDIO/SDA, SDIO/SDT (NTBJPO), USASDC, and NSA. Contractor representatives included BDM International Inc, Beta Analytics Inc, General Electric, MITRE, Martin Marietta, COLSA Inc, and SPARTA.

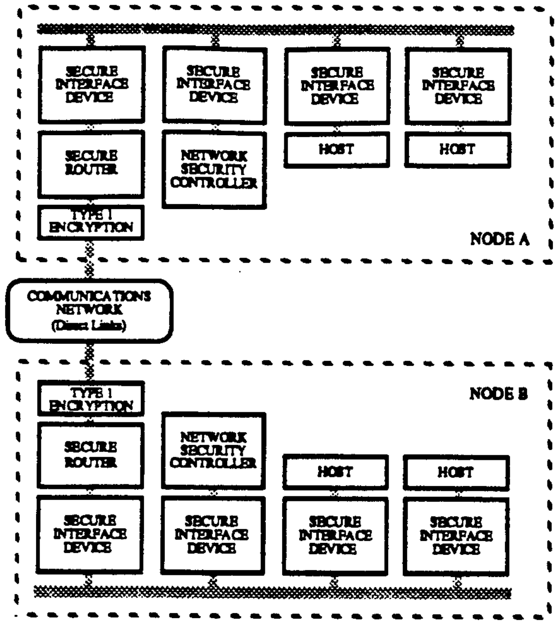
The Tiger Team determined that the need for security in the NTB environment is dictated by the sensitivity of information and the internal and external threat of compromise of that information. The report concluded that security as such is an enabling technology which provides a wide range of users access to shared communication and computing resources which process information at multiple levels of classification. The challenge in providing the needed security is defined by the environment within which the NTB mission must be performed. The key elements of the mission environment include:

a. Geographically dispersed sites with many different AIS platforms and numerous communications requirements;

b. A wide range of users from the Government, industry, and various U.S. Allies with diverse clearance levels and discretionary access control requirements; and

c. Data with a wide range of security classification levels, multiple categories and several COIs.

The report included system level requirements and alternative architectures, operational concepts, and implementation approaches that were evaluated based upon their projected cost and responsiveness to the system level requirements. The Tiger Team's report concluded that establishment of MLS networks is now a realistic alternative to the continued proliferation of single-level networks. Two architectures were recommended, architecture 1 and architecture 3. Architecture 1 provides direct point-to-point connectivity between sites, whereas architecture 3 uses packet switching. Architecture 1, shown in Figure I-1, was recommended for the near term by the Tiger Team because it provides high communications throughput and can be implemented now using commercial products which use open systems protocols. The Tiger Team's report recommended that implementation flexibility would be maintained by sequencing a prototype acquisition phase that begins at the LAN level and progresses up through the router/gateway level to the backbone network level. This would retain the option to migrate to Architecture 3, shown in Figure I-2, at the router/gateway level should future commercial and Government developments merit this approach.



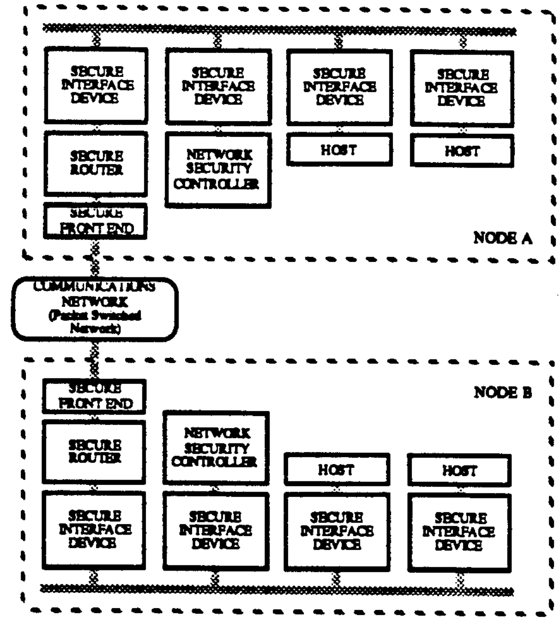


Figure I-1 Architecture 1: Direct Connectivity Figure I-2 Architecture 3: Packet Switching

C. References

(1) CSC-STD-003-85, Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, June 25, 1985

(2) CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, June 25, 1985

(3) DOD Directive 5200.28, Security Requirements for Automated Information Systems, March 21, 1988

(4) DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985

(5) NCSC-TG-005 (Version 1), Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, July 31, 1987

(6) SDIO Directive 5206, Automated Information Systems (AIS) Security Program, September 1991

(7) SDIO Guideline 5206-G, Automated Information Systems (AIS) Security Guidelines, September 1991

(8) SDIO Manual 5206-M, Automated Information Systems (AIS) Security Manual, September 1991

II. DEFINITIONS

In order to provide the mechanism to ensure a consistent presentation of ideas throughout this document the following terms have been given strict definitions.

(1) Automated Information System (AIS)

A set of computer hardware, software, and procedures used to perform a specified function. Examples include mainframes, servers, workstations, terminals, printers, and sets of these elements.

(2) Community of Interest (COI)

A group of persons and/or systems with authorized access to a set of information. A security label is associated (either explicitly or implicitly) with each set of information which identifies the hierarchical classification and the non-hierarchical category(ies) of the information in that set. The hierarchical component of the label represents the classification level of the data and indicates the level of damage resulting from the acquisition of the information by unauthorized personnel. The non-hierarchical component of the label provides a mechanism for restricting access to a subset of those persons authorized access to all information at the given hierarchical security level. Persons or systems that belong to a COI group are permitted to communicate with each other, but are precluded from communicating with persons or systems that do not belong to that COI group. A clearance or access authorization is associated with each user and group of users.

(3) National Test Bed (NTB)

The AIS equipment and its environment that are used to support the SDI Program research and development (R&D) effort. These assets may be connected to the National Test Bed Network.

(4) NTB Network (NTBN)

The communication and control medium that permits connection between NTB AIS assets. It can also be thought of as being bounded by the last electronic connection of any NTB AIS that can communicate with any other NTB AIS.

(5) NTBN Node

The AIS equipment and its environment at a particular physical location that is used to support the NTB and is connected to the NTBN. (e.g., the NTF, USA SDC).

(6) National Test Facility (NTF)

The AIS equipment, and its environment at Falcon Air Force Base, that is used to support the NTB. The NTF acts as the hub for NTBN communications.

III. NEED FOR MLS COMMUNICATIONS AND COMPUTING ENVIRONMENT

Within the National Test Bed, there is a need to provide an MLS operational environment such that Organizational Conflict of Interest (OCI) needs can be met and a mix of U.S. and Allied users with a wide range of clearances can share computing resources and information at multiple levels of security and multiple categories while maintaining separation in accordance with mandatory and discretionary access control requirements. Current technology will not fully support "keyboard to database" MLS operations due to the lack of sufficiently trusted (beyond A1) MLS operating systems, applications, and database management systems.

Levels of trust range from D (Minimal Protection System) to A1 (Verified Design System) where A1 is the highest level of trust currently defined. Levels of trust beyond A1 would be necessary to provide the assurance that an MLS Network with uncleared users and data sensitivities up to Top Secret with multiple categories did not present significant risks. Until levels of trust beyond A1 are defined and attainable, the minimum user clearance must be higher than uncleared and/or the maximum data sensitivity must be lower than Top Secret with multiple categories to keep the risk at an acceptable level.

First generation MLS networks are however achievable using A1 evaluated components to begin the evolutionary process of developing an MLS Network that will be capable of meeting all NTB user needs in the long term. As additional trusted components become available, they can be integrated into the MLS Network to more fully satisfy NTB user needs. As security components with levels of trust beyond A1 are developed and MLS operating systems and applications are developed they can be integrated into the NTBN and NTBN nodes to provide MLS access to NTB resources and data.

IV. EVOLUTIONARY APPROACH

The system high NTBN and dedicated and system high NTBN nodes which are currently capable of transferring and processing data at the Secret/CW level with all users cleared to the Secret/CW level using dedicated mode AISs shall evolve to the MLS mode network capable of transferring and processing data at sensitivities ranging from Unclassified to Top Secret with multiple categories while supporting both cleared and uncleared users using a mix of dedicated, system high, and MLS mode AISs. This evolution will be accomplished in three phases.

Although the COI separation and minimum user clearances and corresponding required level of trust goals for each phase are established, early implementation of individual security features such as MLS operating systems and applications will occur as they become available for the various AISs.

A. Near Term

In the first phase (near term: FY 92-93), the NTF LAN shall be upgraded to MLS mode with the ability to support users with a minimum clearance of Secret communicating and processing data with sensitivities up to Secret with multiple categories (PROPIN, WNINTEL, NOCONTRACT, CNWDI, and ORCON).

The first phase of the evolution shall be accomplished by the addition of MLS security components to control the flow of data to and from individual AISs and groups of AISs at the NTF. NTF AISs (e.g., mainframes and groups of mainframes, workstations and groups of workstations) shall have the ability to support users operating in any one of several COIs. The COI supported by each NTF AIS shall be independent of the COI supported by the other NTF AISs. All other NTBN nodes shall support users operating in the same, single, COI. NTF AISs will be able to exchange data with other NTF AISs and with the other NTBN nodes in accordance with the security policy. Since all nodes, except the NTF, will be supporting users operating in the same single COI, there is no need to control the exchange of data between NTBN nodes during this phase. Therefore, in the near term, security components will only be needed at the NTF. In the near term, the security components shall provide at least a B2 level of trust when evaluated using Appendix A and C of the TNI.

During this phase, the feasibility, utility, ease of use, and performance characteristics of the MLS security components and their effect on operations shall be evaluated through prototyping, to provide a basis for refinement of the near, mid, and long term requirements.

B. Mid Term

In the second phase (mid term: FY93-95), the NTBN shall be upgraded such that each NTBN node can support users operating in a COI which is independent of the COI supported by any of the other nodes. The MLS mode of operation will be extended from the NTF LAN out to the point where each NTBN node connects to the NTBN. In this phase, the NTBN and NTBN nodes shall have the capability to support users with a minimum clearance of Secret and to control access to data up to the Top Secret level with multiple categories (PROPIN, NOFORN, REL, WNINTEL, CNWDI, ORCON, and NOCONTRACT). In the mid term, the security components shall provide at least a B3 level of trust when evaluated using Appendix A and C of the TNI.

The second phase shall be accomplished by the addition of security components to individually control the flow of data to and from each NTBN node. At the end of the second

phase, the NTBN will operate in the MLS mode with a combination of dedicated, system high, and MLS mode nodes supporting users operating in multiple independent COIs.

C. Long Term

In the third phase (long term: FY96-99), some of the NTB AISs, such as the NTF CRAY, IBM, and VAX mainframes and user workstations, shall be upgraded to MLS mode using MLS operating systems and applications that are trusted to segregate information within an AIS based upon data sensitivities. This will allow NTB users operating in differing COIs to fully share the NTB computing resources. In the long term, the security components shall provide at least an A1 level of trust when evaluated using Appendix A and C of the TNI.

In this phase, the security components will control the access of both cleared and uncleared users to data with sensitivities up to Top Secret with multiple categories. The recommended level of trust for such a network is beyond the state of current computer security technology. The recommended minimum user clearance and maximum data sensitivities for an A1 level of trust are shown in Tables VI-4 and VI-5. However, the Designated Approving Authority (DAA) may authorize operation with lesser user clearances and/or greater data sensitivities. In addition, as higher levels of trust become achievable, the allowable minimum user clearance and/or maximum data sensitivity can be revised.

In the third phase, as MLS operating systems, database management systems, and applications become available for the NTB AISs, they will be able to support concurrent use of NTB computing resources (e.g., servers, workstations, and CRAY, IBM, and VAX mainframes) by users operating in different COIs. Users will be able to share computing resources, data in databases, and names on name servers, and to more easily exchange electronic mail.

The MLS NTF LAN, NTBN, and AISs will serve as models for the other nodes supporting the SDI mission. The network security architectures and security components used on the NTF LAN and the secure operating systems and applications on the MLS NTF AISs could be replicated throughout the NTBN nodes to increase the sharing of SDI communication and computing resources. The selection and implementation of MLS capabilities at each of the nodes will be the responsibility of the managers of those nodes.

V. REQUIREMENTS

This section contains the functional, performance, and security requirements for the security components for the near, mid, and long terms

A. Requirements Applicable To All Phases

1. Functional Requirements

The security components shall:

(1) Allow the transfer of information between AISs only if the transfer does not violate the security policy enforced by those components.

(2) Allow the transfer of information between NTBN nodes only if the transfer does not violate the security policy enforced by those components.

(3) Provide the capability to establish and change the set of COIs and to identify the current COI supported by AISs and NTBN nodes.

(4) Provide the capability to increase or decrease the number of AISs at a node and the NTBN nodes connected to the NTBN without requiring a complete reaccreditation.

(5) Provide the capability for single level AISs to support users operating in one of several COIs.

(6) Provide centralized network security management.

2. Performance Requirements

The security components shall:

(1) Not increase communications error rates above 1 in 10^{12} (To Be Resolved TBR)) for data transfers between AISs, between AISs and NTBN nodes, and between NTBN nodes.

(2) Not reduce communications availability between AISs, between AISs and NTBN nodes, and between NTBN nodes below 99.95 (TBR) percent.

(3) Not degrade communication bandwidths between AISs, between AISs and NTBN nodes, and between NTBN nodes by more than 5 (TBR) percent.

3. Security Requirements

The security components shall:

(1) Be developed and maintained in a "closed" security environment as defined in CSC-STD-003-85.

(2) Implement RFC-1038, Draft Revised IP Security Option (RIPSO).

(3) Provide the capability for AISs and NTBN nodes supporting users operating in the same and differing COIs to use the same communications path.

(4) Meet the security requirements in the following documents:

a. SDIO Directive 5206, Automated Information Systems (AIS) Security Program, September 1991

b. SDIO Guideline 5206-G, Automated Information Systems (AIS) Security Guidelines, September 1991

c. SDIO Manual 5206-M, Automated Information Systems (AIS) Security Manual, September 1991

d. DOD Directive 5200.28, Security Requirements for Automated Information Systems, March 21, 1988

e. DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985

f. CSC-STD-003-85, Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, June 25, 1985

g. CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, June 25, 1985

h. NCSC-TG-005 (Version 1), Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, July 31, 1987

B. Near Term Requirements

The security components shall provide the capability for the exchange of data in multiple COIs among NTF AISs and between NTF AISs and NTBN nodes operating in the same COI. In this phase, the NTF LAN will transition to the MLS mode of operation. While the NTF LAN will be MLS in this phase, all of the other NTBN nodes will remain in the system high or dedicated mode and support users operating in the same single COI. In this phase, the COI supported by all NTBN nodes other than the NTF will be identical.

1. Functional Requirements

The security components shall:

(1) Control the simultaneous transfer of data among NTF AISs and between NTF AISs and the other NTBN nodes at the following security levels: Unclassified, Unclassified Sensitive, Confidential, and Secret with or without the following releasability markings: PROPIN, WNINTEL, NOCONTRACT, ORCON, and CNWDI.

(2) Provide the capability to obtain, store, display, and change the security parameters necessary to control the transfer of information among NTF AISs and between NTF AISs and the other NTBN nodes.

(3) Provide the capability to collect and display data and control information transferred among NTF AISs and between NTF AISs and the other NTBN nodes.

(4) Provide the capability to support users operating in one of several COIs as a COI group on all of the NTBN nodes.

2. Security Requirements

The security components shall:

(1) Have sufficient level of trust to permit the minimum required user clearance to be Secret.

(2) As a minimum, meet the class B2 level of trust requirements defined in DOD 5200.28, DOD Trusted Computer Security Evaluation Criteria (TCSEC). A1 security components shall be used if available.

(3) As a minimum, meet the class B2 level of trust requirements defined in NCSC-TG-005, Trusted Network Interpretation (TNI) of the TCSEC when evaluated as described in Appendix A and C of the TNI.

C. Mid Term Requirements

The security components shall provide the capability for NTF AISs, NTF AISs and NTBN nodes, and NTBN nodes to simultaneously exchange data in several COIs. In this phase, each NTBN node will have the capability to support users operating in a COI which is independent of the COI of any other NTBN node or any NTF AIS.

1. Functional Requirements

The security components shall:

(1) Control the simultaneous transfer of data among NTF AISs, between NTF AISs and other NTBN nodes, and between NTBN nodes at the following security levels: Unclassified, Unclassified Sensitive, Confidential, Secret and Top Secret with or without the following releasability markings: NOFORN, REL, WNINTEL, CNWDI, ORCON, NOCONTRACT, and PROPIN.

(2) Provide the capability to obtain, store, display, and change the security parameters necessary to control the transfer of data among NTB AISs, between NTB AISs and other NTBN nodes, and among NTBN nodes.

(3) Provide the capability to collect and display data and control information transferred among NTB AISs, between NTB AISs and other NTBN nodes, and among NTBN nodes.

(4) Provide the capability for each NTBN node to support users operating in one of several COIs.

(5) Provide the capability for each NTBN node to support users operating in different COIs.

2. Security Requirements

The security components shall:

(1) Have sufficient level of trust to permit the minimum required user clearance to be Secret.

(2) As a minimum, meet the class B3 level of trust requirements defined in DOD 5200.28, DOD Trusted Computer Security Evaluation Criteria (TCSEC). A1 security components shall be used if available.

(3) As a minimum, meet the class B3 level of trust requirements defined in NCSC-TG-005, Trusted Network Interpretation (TNI) of the TCSEC when evaluated as described in Appendix A and C of the TNI.

D. Long Term Requirements

The security components shall provide the capability for users operating in multiple COIs to share NTB computing resources and databases and for NTB AISs, NTB AISs and other NTBN nodes, and other NTBN nodes to exchange data in multiple COIs. In this phase, some AISs will transition to MLS mode. This will enable users with a wide range of clearances to process, store, and access data in multiple COIs, simultaneously, on a single AIS.

1. Functional Requirements

The security components shall:

(1) Control the simultaneous processing and transfer of data at the following security levels: Unclassified, Sensitive, Confidential, Secret, and Top Secret with or without any or all of the following releasability markings: NOFORN, REL, CNWDI, WNINTEL, ORCON, NOCONTRACT, PROPIN, SIOP, and SIOP-ESI.

(2) Provide the capability to obtain, store, display, and change the security parameters necessary to control the transfer of data among NTB AISs, between NTB AISs, other NTBN nodes, and among NTBN nodes, and within MLS AISs.

(3) Provide the capability to collect and display data and control information transferred among NTB AISs, between NTB AISs and other NTBN nodes, and among NTBN nodes, and within MLS AISs.

(4) Provide the capability to establish and change the set of COIs and the current COI that users of shared MLS NTB computing resources operate in.

(5) Provide the capability to increase and decrease the number of MLS NTB computing resources without affecting the security of the NTBN.

(6) Provide the capability for an NTB AIS to support users operating in several COIs, simultaneously.

2. Security Requirements

The security components shall:

(1) Have sufficient level of trust to permit the minimum required user clearance to be Uncleared.

(2) Provide the capability for NTB MLS AISs, NTB non-MLS AISs, and NTBN nodes operating in differing COIs to use the same communications path.

(3) As a minimum, meet the class A1 level of trust requirements defined in DOD 5200.28, DOD Trusted Computer Security Evaluation Criteria (TCSEC).

(4) As a minimum, meet the class A1 level of trust requirements defined in NCSC-TG-005, Trusted Network Interpretation (TNI) of the TCSEC when evaluated as described in Appendix A and C of the TNI.

(5) Provide the capability for MLS AISs to support users operating in multiple COIs, concurrently.

VI. SECURITY ARCHITECTURE

This section defines the modes of operation, risk indexes, "open" versus "closed" environments, and presents the near, mid, and long term security architectures which support evolution from the existing system high NTBN and dedicated and system high NTBN nodes to the MLS mode network.

A. Modes of Operation

AISs may be operated in one of several modes, including: dedicated, system high, multilevel, controlled, and compartmented. These modes are defined in CSC-STD-003-085 as follows:

(1) Dedicated

A dedicated mode system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

(2) System High

A system high mode system is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system, and all system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.

(3) Controlled

A controlled mode system is a type of multilevel mode security in which a more limited amount of trust is placed in the hardware/software of the system, with resultant restrictions on the classification levels and clearance levels that may be supported.

(4) Compartmented

A compartmented mode system is allowed to process more than two or more types of compartmented information (information requiring a special authorization) or any one type of compartmented information with other than compartmented information. In this mode, system access is secured to at least the Top Secret level, but all system users need not necessarily be formally authorized access to all types of compartmented information being processed and/or stored in the system.

(5) Multilevel

A multilevel mode system allows two or more classification levels of information to be processed simultaneously within the same system when users are not cleared for all levels of information present.

The modes, as listed above, can be thought of as being hierarchical in that each succeeding mode provides a superset of the protections provided by the mode before it in the list.

Also, it is generally more difficult, and expensive, to implement each succeeding mode. Therefore, the "lowest" mode which will provide the required protection should be selected unless there is some reason to select a "higher" mode.

The NTBN will transition from system high and the NTBN nodes will transition from dedicated and system high mode to MLS mode in response to mission requirements as shown in Table VI-1.

Modes of Operation in Each Phase

	Near Term	Mid Term	Long Term
MLS Network	MLS*	MLS	MLS
NTBN	System High	MLS	MLS
NTF LAN	MLS	MLS	MLS
Other NTBN Nodes (NTBN nodes other than the NTF)	Dedicated and System High (All users supported in a single COI)	Dedicated and System High (Each other NTBN node has the potential to support users operating in a COI which is different from the COI supported by any other node)	Dedicated, System High, and MLS
NTB AISs at the NTF	Dedicated and System High (Some support users operating as part of a COI group and others operate independently with respect to COI)	Dedicated and System High (Some support users operating as part of a COI group and others operate independently with respect to COI)	Dedicated, System High, and MLS

* Note: In the near term, the MLS Network operates in the MLS mode because a portion of the system, the NTF LAN, operates in the MLS mode. The NTBN remains in the system high mode since all of the other NTBN nodes continue to operate as a group in a single COI. In the mid term, the NTBN transitions to MLS when each of the other NTBN nodes can operate in a different COI.

Table VI-1

In the near term, there is a need to store and control classified and unclassified proprietary data belonging to multiple contractors and classified and unclassified SDI data. Data can be labeled using proprietary designators that indicate which contractor, if any, is the "owner" of that data. The existing system high and dedicated mode of operation can not segregate data on the basis of proprietary labels, or any other security designators. Multilevel mode is the "minimum" mode that will segregate users based upon proprietary designators. Therefore, during the near term, the operational mode of the MLS Network should transition from system high , processing data at the Secret/CW level to MLS, processing data at the Unclassified, Unclassified Sensitive, Confidential, and Secret levels with multiple categories.

In the near term, individual NTBN nodes and AISs, and groups of NTBN nodes and AISs, will be operating in either the system high, dedicated, or MLS mode. As shown in Table VI-1, in the near term, the NTF LAN will operate in the MLS mode. All nodes, other than the NTF, will support users operating only in the same single COI. Some of the NTF AISs will support users operating as a COI group in the same single COI. Others will support users operating in a COI which is independent of the COI supported by other NTF AISs.

It is essential that the high speed "backside" hyperchannel links between the NTF mainframes (e.g., CRAYs, IBMs, VAXs) be made switchable to allow each mainframe's users to operate in a COI which is independent of the COI supported by other mainframes. The capability must be provided to logically or physically remove the "backside" connections between mainframes supporting users operating in different COIs. Since there are no evaluated high speed products available now to provide logical separation, switches will need to be added to physically segregate the mainframes by COI.

In the mid term, the other NTBN nodes will gain the capability to support users operating in a COI which is independent of the COI supported by any of the other nodes. This will allow individual nodes supporting users operating in different COIs to share the NTBN, simultaneously. Each NTBN node (other than the NTF which will already be MLS) will continue to operate in system high or dedicated mode.

In the long term, some of the AISs will transition to MLS mode through the addition of MLS operating systems and applications. Once this is accomplished, NTB users operating in separate COIs will gain the capability to share NTB computing resources. High speed secure gateways should be available during this phase to allow replacement of the "backside" hyperchannel switches. This will automate the transitions between various groupings of AISs into COIs.

B. Risk Index

Classified data must be protected against access by persons not having sufficient clearance and need-to-know. The first step in determining the recommended minimum level of trust of an AIS required to protect classified data is the determination of the system's risk index. Risk index (RI) is defined by CSC-STD-003-85 as the disparity between the minimum clearance or authorization of system users (R_{min}) and the maximum sensitivity of data (R_{max}) processed by the system. Table VI-2 shows the calculated risk index ($RI = R_{max} - R_{min}$) associated with a system's minimum user clearance and maximum data sensitivity. The higher the risk index, the higher the recommended level of trust. The recommended minimum level of trust, as shown in Table VI-3, is also dependent upon whether a system is developed and maintained in an "open" or "closed" environment.

For the near term , the minimum user clearance will be Secret and the maximum data sensitivity will be Secret with multiple categories (S_{mc}). Therefore, the risk index (R_{max} - R_{min}) as shown in Table VI-2 is 2 and the recommended minimum level of trust for a "closed" environment as shown in Table VI-3 is B2. In the mid term, the minimum user clearance will be Secret and the maximum data sensitivity will be Top Secret with two or more categories (PROPIN, NOFORN, WNINTEL, CNWDI, etc.) Therefore, the risk index as shown in Table VI-2 is 4 and the recommended minimum level of trust for a "closed" environment as shown in Table VI-3 is B3.

Risk Index

Maximum Data Sensitivity (R_{max}[a])

R_{min}[b]	U 0	N 1	N_{mc} 2	C 2	C_{mc} 3	S 3	S_{1c} 4	S_{mc} 5	TS 5	TS_{1c} 6	TS_{mc} 7
0	0	1	2	2	3	3	4	5	5	6	7
1	0	0	1	1	2	2	3	4	4	5	6
2	0	0	0/1[c]	0	1	1	2	3	3	4	5
3	0	0	0/1[c]	0	0/1[c]	0	1	2	2	3	4
4	0	0	0/1[c]	0	0/1[c]	0	0/1[c]	1	0	2	3
5	0	0	0/1[c]	0	0/1[c]	0	0/1[c]	0/1[c]	0	1	2
6	0	0	0/1[c]	0	0/1[c]	0	0/1[c]	0/1[c]	0	0/1[c]	1
7	0	0	0/1[c]	0	0/1[c]	0	0/1[c]	0/1[c]	0	0/1[c]	0/1[c]

Notes:

a. R_{max} - Maximum Data Sensitivity: U = Unclassified, N = Unclassified but Sensitive , N_{mc} = Unclassified but Sensitive with multiple categories, C = Confidential, C_{mc} = Confidential with multiple categories (Note that C_{1c} is not defined), S = Secret, S_{1c} = Secret with one category, S_{mc} = Secret with multiple categories, TS = Top Secret, TS_{1c} = Top Secret with one category, TS_{mc} = Top Secret with multiple categories.

b. R_{min} - User Clearance or Authorization: 0 = Uncleared, 1 = Not cleared but authorized access to sensitive unclassified information, 2 = Confidential, 3 = Secret, 4 = Top Secret with a Background Investigation, 5 = Top Secret with a Special Background Investigation, 6 = Top Secret with Authorization for 1 Compartment, 7 = Top Secret with Authorization for Multiple Compartments.

c. If R_{min} is greater than or equal to R_{max} and there are categories to which some users are not authorized access, then the risk index is 1.

Table VI-2

Recommended Minimum Level of Trust[2]

Risk Index	Security Operating Mode	"Open" Environment	"Closed" Environment
0	Dedicated	No Prescribed Minimum	No Prescribed Minimum
0	System High	C2	C2
1	Limited Access, Controlled, Compartmented, Multilevel	B1	B1
2	Limited Access, Controlled, Compartmented, Multilevel	B2	B2
3	Controlled, Compartmented, Multilevel	B3	B2
4	Multilevel	A1	B3
5	Multilevel	*	A1
6	Multilevel	*	*
7	Multilevel	*	*

(* = Beyond A1)

Table VI-3

[2]CSC-STD-003-85, Table 3 on page 12

In the long term, the minimum user clearance will be "U" and the maximum data sensitivity will be Top Secret with two or more categories. Therefore, the risk index is 7 and the recommended minimum level of trust is "beyond A1". At the A1 level of trust for a "closed" environment if uncleared users are supported, the maximum data sensitivity level recommended would be Top Secret with no categories. Similarly, to support a maximum data sensitivity of Top Secret with multiple categories the minimum user clearance would have to be Confidential.

C. "Open" vs. "Closed" Environments

AISs may be developed and maintained in either "open" or "closed" environments. Tables VI-4 and VI-5 show the relationship among the type of environment, the maximum data sensitivity processed by a system, the minimum security clearance of users of that system, and the minimum criteria class (level of trust) required. For example, in an "open" environment system, where the maximum data sensitivity is Secret with one category and the minimum clearance held by any user is Confidential, an A1 level of trust as defined in DOD 5200.28 (The "Orange" book) is required. However, in a closed environment, a B3 level of trust is required. Accreditation may be achieved with lesser levels of trust than those recommended if the DAA believes there is a rational reason to accept the added risk. For example, the risk may be mitigated by additional security constraints provided through physical, administrative, and/or personnel security.

In an "open" environment, **either** of the following statements is true. In a "closed" environment, **both** of the following statements are true.

(1) Applications developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of the data to be processed is Confidential or less, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of the data is Secret or above, developers have at least a Secret clearance.

(2) Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of applications.

Since some of the software and virtually all of the hardware will not be developed by sufficiently cleared personnel, an "open" environment will result unless additional security measures are implemented. Available secure interface units may not have the requisite level of trust to meet the minimum user clearance and maximum data sensitivity requirements in an "open" environment. However, these security interface units would have sufficient trust in a "closed" environment. The conversion from an "open" to a "closed" environment could be accomplished procedurally by requiring that all hardware and software developed outside the environment be reviewed by sufficiently cleared personnel prior to its use. The reviewers must be cleared to at least the Secret (TBR) level. Also, once it has been reviewed and approved for use, it may not be accessed by insufficiently cleared personnel in any way that could result in its modification.

D. Near Term

AISs may be connected to a security device in such a way as to support users operating in a single COI or in multiple COIs, as shown in Figure VI-1. Some NTF AISs will always support users operating in the same COI as other NTF AISs. These NTF AIS may share a

Level of Trust Required in an "Open" Environment[3]

Maximum Data Sensitivity
"Open" Environment

Minimum Clear- ance	U	N	C	S	TS	1C	MC
U	C1	B1	B2	**B3**	*	*	*
N	C1	C2	**B2**	B2	**A1**	*	*
C	C1	C2	C2	B1	**B3**	**A1**	*
S	C1	C2	C2	C2	B2	**B3**	**A1**
TS(BI)	C1	C2	C2	C2	C2	B2	**B3**
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[a]	B1[b]
MC	C1	C2	C2	C2	C2	C2[a]	C2[a]

Table VI-4

Level of Trust Required in a "Closed" Environment[4]

Maximum Data Sensitivity
"Closed" Environment

Minimum Clear- ance	U	N	C	S	TS	1C	MC
U	C1	B1	B2	**B2**	**A1**	*	*
N	C1	C2	**B1**	B2	**B3**	**A1**	*
C	C1	C2	C2	B1	**B2**	**B3**	**A1**
S	C1	C2	C2	C2	B2	**B2**	**B3**
TS(BI)	C1	C2	C2	C2	C2	B2	**B2**
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[a]	B1[b]
MC	C1	C2	C2	C2	C2	C2[a]	C2[a]

Table VI-5

Notes:

a. The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of the current technology. Such environments must augment technical protection with physical, personnel, and/or administrative safeguards.

b. It is assumed that all users are authorized access to all categories present system. If some users are not authorized for all categories, then a class B1 level of trust or higher is required.

c. Where there are more than two categories, at least a B2 level of trust is required.

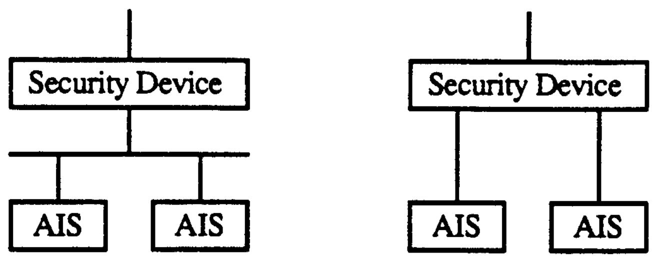
d. The differences between the tables are in bold.

[3] CSC-STD-004-85, Table 5, Page 13.

[4] CSC-STD-004-85, Table 7, page 21.

LAN connection to the security device. Some NTF AISs will support users operating in different COIs than other NTF AISs. Each of these NTF AISs must directly connect to the security device.

AIS to Security Device Connectivity



AISs Must Operate In the Same Community Of Interest

AISs May Operate In Different Communities Of Interest

Figure VI-1

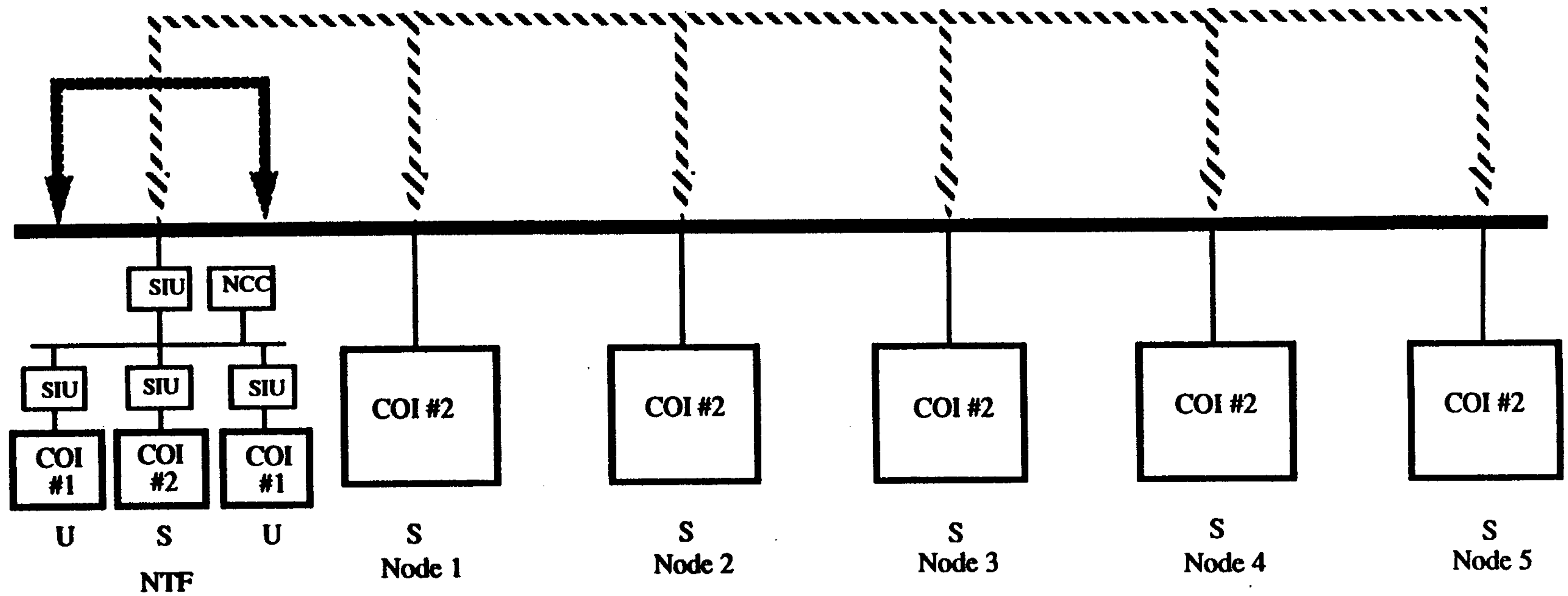
The present NTBN architecture is a "bursted star" with the NTF as the hub. The architectures shown below build upon that structure by inserting secure interface units to control the flow of data among NTBN nodes and NTF AISs. The architectures shown below are responsive to the requirements and provide a framework for the use of current computer security components to provide an MLS mode of operation at the NTF LAN level in the near term with evolution to an MLS mode of operation on the NTBN and at the NTBN nodes with an A1 level of trust.

As shown in Figure VI-2, the near term security architecture provides the capability for NTF AISs connected by an MLS LAN to exchange data with other NTF AISs and for NTF AISs to exchange data with the other NTBN nodes based upon COI. Secure Interface Units (SIU) (e.g., Boeing Secure Network Servers (SNS)) and the Network Control Center (NCC) (e.g., Boeing Network Manager (NM)) control the transfer of data among NTF AISs and between NTF AISs and the other NTBN nodes. The NTF LAN operates in the MLS mode and supports multiple COIs. The other NTBN nodes support users operating in the same single COI. The SNSs ensure that data is not transferred to an NTF AIS or NTBN node unless the transfer is in accordance with the security policy.

The NCC manages the security tables and stores the audit data for the SIUs. In this phase, the NCC only needs to be connected to the NTF LAN since that is the extent of the MLS domain.

E. <u>Mid Term</u>

As shown in Figure VI-3, the mid term security architecture provides the capability for each of the NTBN nodes to support users operating in different COIs and for the NTF LAN to continue to support users operating in multiple COIs. In the mid term phase, the NTF AISs and each of the other NTBN nodes can support users operating in a COI which may be different than the COI supported by other AISs and nodes. The SIUs ensure that data is not transferred to an NTF AIS or NTBN node unless the transfer is in accordance with the security policy.



- NTF AISs operating in the same COI can exchange data
- All other NTBN nodes operate in the same community of interest
- NTBN nodes can exchange data with those NTF AISs operating in the same COI
- Network Control Center (NCC) manages Secure Interface Units (SIUs) at the NTF
- Minimum User Clearance: Secret
- Maximum Data Sensitivity: Secret / Multiple Categories

Figure VI-2 Near Term Security Architecture
B2 Level of Assurance as a Minimum

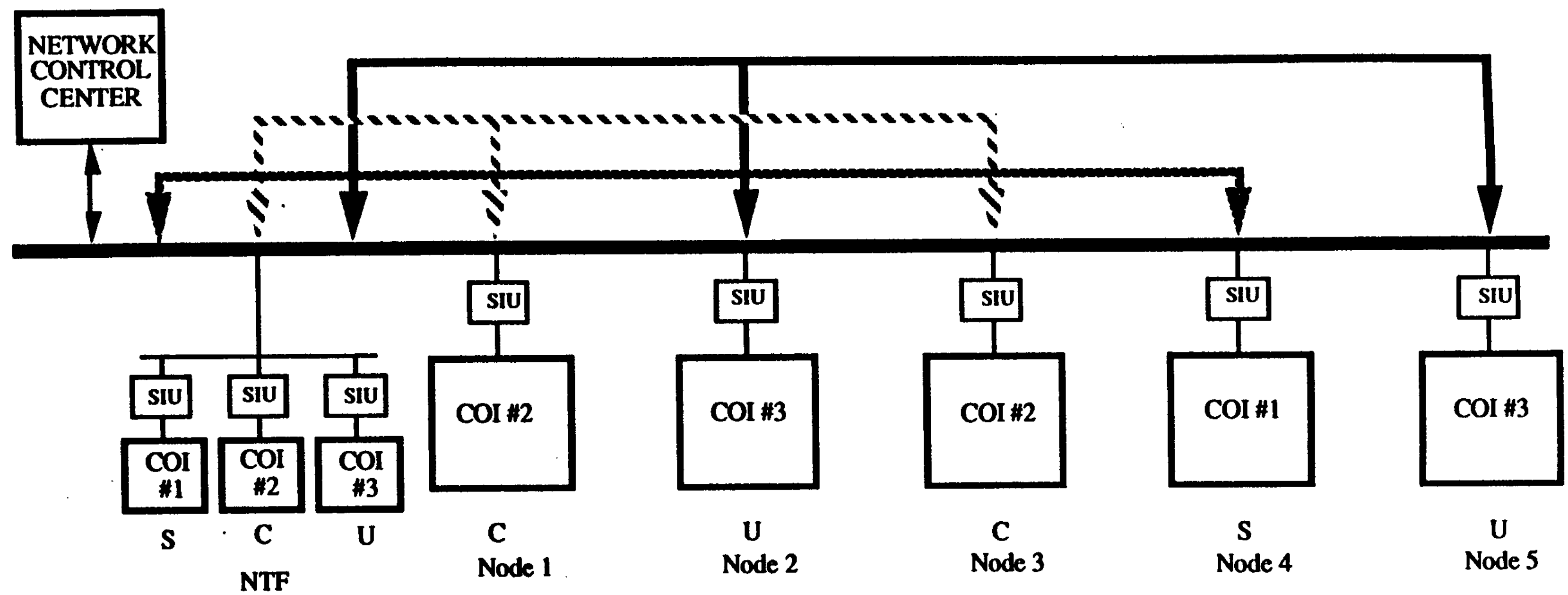
The network control center manages the security tables and stores the audit data for the SIUs. The network control center is connected to the NTBN to allow it to control the secure interface units on each NTBN node's connection to the NTBN.

NTBN nodes are currently connected to the NTF by a combination of Type 1 encryption units and leased T1 land lines. All data is transmitted to the NTF regardless of its ultimate destination. If secure high speed (T1 or T3) packet switch interface devices and data paths are available, there is the potential for the transition of some node to node communications to packet switching technology during the mid term. This would reduce the amount of traffic transiting the NTF and make the network less susceptible to a complete failure due to an NTF outage.

F. Long Term

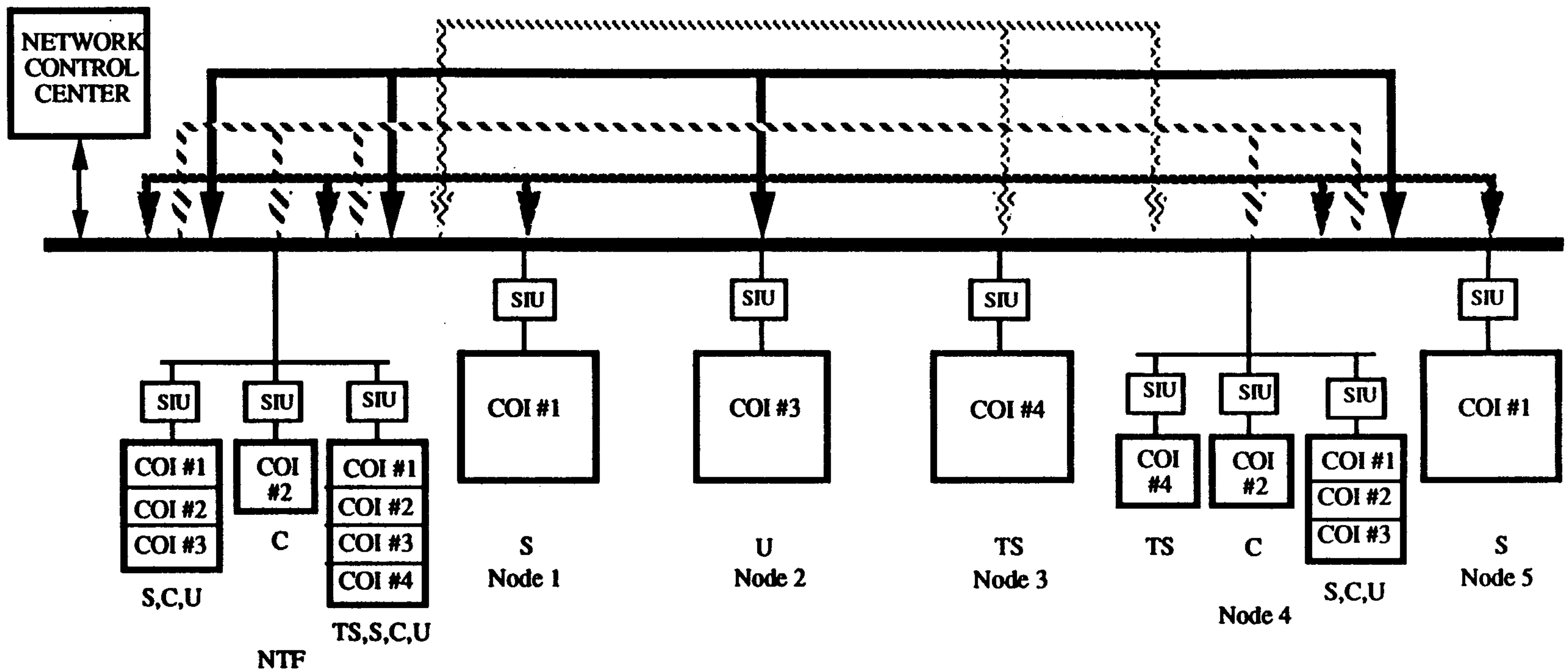
As shown in Figure VI-4, the long term security architecture provides the capability for NTBN nodes to support users operating in differing COIs to share the computing resources and communication media and for nodes supporting users operating in the same COI to exchange data.

MLS AISs provide the capability for users to share computing resources. Those MLS AISs that implement the SNS functions will not require an SNS. There is the potential for proliferation of security features (e.g., MLS operating systems and applications at the NTF) to other NTBN nodes.



- NTBN nodes operating in multiple COIs
- NTBN nodes operating in the same COI can exchange data.
- NTF node operates MLS and therefore can exchange data with and provide processing support to other nodes in the same COI
- NCC manages SIUs for all nodes
- Minimum User Clearance: Secret
- Maximum Data Sensitivity: Top Secret / Multiple Categories

Figure VI-3 Mid Term Security Architecture
B3 Level of Assurance as a Minimum



• NTF AISs operate in MLS mode and can exchange data with and provide processing support to those NTBN nodes and AISs operating in the same COI.
• Potentially some NTBN nodes operate MLS and AISs at those nodes can exchange data with NTF AISs and other nodes in the same COI

• Minimum User Clearance:	Uncleared	or	Confidential
• Maximum Data Sensitivity:	Top Secret		Top Secret/ Multiple Categories

Figure VI-4 Long Term Security Architecture

A1 Level of Assurance as a Minimum

VII. PRELIMINARY IMPLEMENTATION ARCHITECTURES

Presently, the NTBN is operated in the system high mode at the Secret/CW security level. All data is treated as if labeled at the Secret/CW level and all users have at least a Secret/CW security clearance. There is a requirement to allow users operating in several COIs to share some of the computing and communication resources of the NTB.

This section presents preliminary implementation architectures for the near, mid, and long terms to satisfy this need. While the figures include identification of specific equipments and their interconnection, there may be other equipment suites and configurations that have the potential of meeting the requirements. The purpose of this section is to illustrate the use of one set of security interface units to support users operating in several COIs, simultaneously. The actual configuration implemented will be determined by an analysis of many factors such as the availability, cost, functionality, accepted level of trust of secure interface units; the minimum user clearance, acceptable level of risk, range and maximum data sensitivity; and the development and maintenance environments.

A. Near Term

The Tiger Team recommended implementation of MLS LANs connected to a communications network secured by link encryption devices. The evolution of this architecture will begin with the addition of secure interface units and switches at the NTF to allow the NTF LAN to operate in the MLS mode. NTF AISs supporting users operating in the same COI will be able to exchange data. An MLS device installed between the NTF LAN and the other NTBN nodes will allow the other NTBN nodes to operate in a single COI and to exchange data with other NTBN nodes and those NTF AISs that are supporting users operating in the same COI.

The near term MLS capability can be achieved using physical switches, Boeing MLS LAN Secure Network Servers (SNS), and a Boeing Network Manager (NM) as shown in Figure VII-1. The SNSs and switches are shaded in the figure. The switches are required to control the hyperchannel connectivity between the IBM, CRAY, and VAX mainframes to allow them to support users operating in either the same or different COIs as mission requirements dictate. While the figure shows the capability for only three separate COIs, additional switching could provide the capability for more COIs. Also, it may be necessary for the IBM 3090s to support users operating in one COI, the VAXs to support users operating in a second COI, and the CRAYs to support users operating in a third COI. Other switching configurations could provide the capability to set up different COIs groupings from those shown. Procedures will be required to perform "color changes" when the mainframes transition from one COI to another to ensure that no data remains from the first COI.

The SNSs can be trusted to ensure separation between NTBN nodes and AISs supporting users operating in different COIs. SNSs will provide service to individual AISs and groups of AISs on a LAN. Each AIS with an individual connection to an SNS may operate in a separate COI. AISs on a LAN that share a connection to an SNS must operate in the same COI. In addition, the SNS has the capability to perform the one way guard function.

Each SNS can support up to seven ethernet cards or up to 56 RS-232C interfaces. The arrangement and grouping of AISs connected to SNSs will depend upon the physical location of the SNSs and the AISs they service.

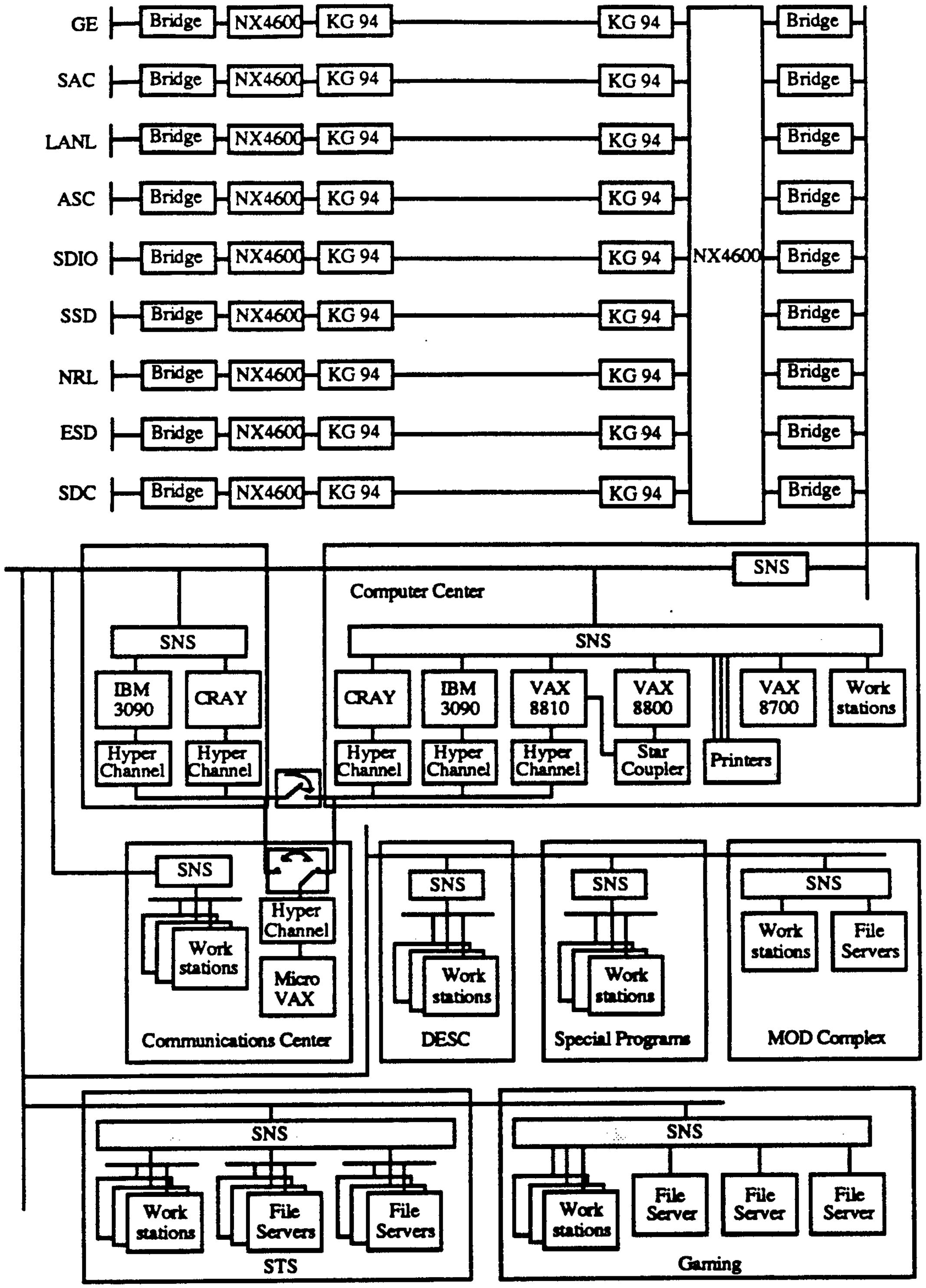


Figure VII-1 Near Term: 1992 - 1993

The Mandatory Access Control and Identification and Authentication components of the Boeing MLS LAN have been evaluated at the A1 level of trust. The NM which includes the Discretionary Access Control and Auditing components, is presently being evaluated at the A1 level by NSA. The SNS and NM are being upgraded to include standard interfaces and improve performance. The revised SNS and NM are presently in the NSA developmental evaluation phase. Testing is scheduled for September through December 1992 and the formal evaluation should be complete by February 1993. Therefore, they should be available (in evaluation) in the near term and will be formally evaluated by the mid term. SNS and NM capabilities are discussed in Attachment I.

B. Mid Term

The mid term goals can be achieved by installing MLS devices as interfaces between each of the NTBN node LANs and the NTBN as shown in Figure VII-2. NTBN nodes and NTF AISs supporting users operating in the same COI will be able to exchange data.

Although each NTBN node will support users operating in a single COI in the mid term, all NTBN nodes will not necessarily support users operating in the same COI. All data exchanged among nodes is presently processed by the NX4600 at the NTF. The NX4600 is a T1 time division multiplex device. Therefore, if the NX4600 (or other similar device) remains in the communications path, data of multiple COIs may be present in the NX4600 at any given time. It is possible for data from one channel to be sent to the wrong channel due to an NX4600 malfunction. Therefore, Figure VI-3 shows type 1 encryption devices (NESs) to ensure that if data is sent to the wrong channel by the NX4600, that it will be unintelligible to an insufficiently cleared recipient. Type 1 encryption is required because an untrusted device is transferring data of multiple COIs at the same time. There are three type 1 encryption devices (Motorola Network Encryption System (NES), WANG Trusted Interface Unit (TIU), and XEROX Encryption Unit (XEU)) that could be used.

The Motorola NES costs about $12,000, meets SDNS standards, interfaces with the electronic key management center, does not encrypt the IP header, uses an open architecture that reduces evaluation time for new interface cards, and uses the "FIREFLY" encryption algorithm which provides electronic key management. In addition, the enhanced version, due out by the fourth quarter of 1992 will include SNMP and electronic update of configuration tables over the network. The WANG TIU costs about $8600, has 64k buffers on each side, does not encrypt the IP header, and responds to requests for status via 'pings'. The XEROX XEU costs about $6000 and encrypts the IP header. Encryption of the IP header makes the packets unsuitable for internet processing. XEROX has an additional device (a combination of a PC ($1,500) and software ($3,500) that can be added to the communications path to allow use of the IP header over internets. Internetting may, or may not, be a requirement. It will depend upon whether internet networks such as DISNET are used. At present, there is no firm requirement for internet processing of data. Type 1 encryption may not be required after mid term if the NX4600 is replaced by a trusted device or by a device that does not process multiple COIs simultaneously or if type 1 encryption is added to the SNS at a reasonable cost.

The Motorola NES is the recommended solution since it meets SDNS standards, interfaces with the electronic key management center, does not encrypt the IP header, uses an open architecture that reduces evaluation time for new interface cards, and uses the "FIREFLY" encryption algorithm which provides electronic key management. The final decision will depend upon the following factors: need for encryption, requirement for internetting, requirement for SNMP capability, availability of SNS with encryption, and cost. This decision can be delayed until additional data is available since there is no problem until mid term (1993).

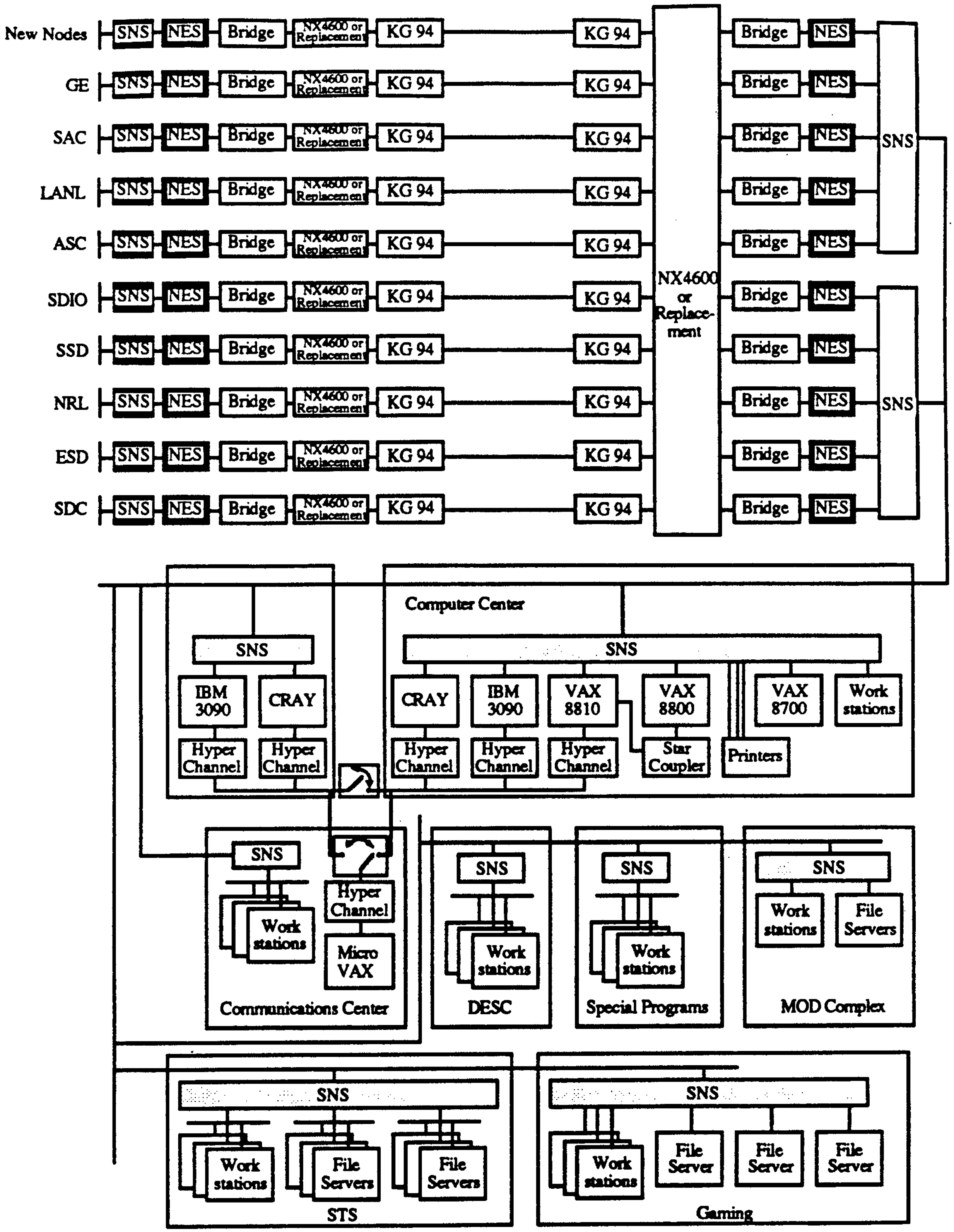


Figure VII-2 Mid Term: 1993 - 1995

C. Long Term

The long term goals can be achieved by installing hardware and/or software that results in MLS AISs as shown in Figure VII-3. The switches on the high speed inter-mainframe busses will be replaced by high speed MLS gateways. This will enable additional flexibility and control over COI groups. The NESs will no longer be required if the SNSs have type 1 encryption by 1996 or if there are no untrusted devices (e.g., NX4600s) processing multiple COIs.

In the long term, the users operating in multiple COIs will have the capability to share the computing resources of the MLS Network using SNSs and MLS hosts and workstations. MLS hosts and workstations will provide the capability for users to operate in several COIs simultaneously and for those users to share databases and processors since MLS hosts and workstations will be trusted to segregate data by COI on a single platform. Not all of the NTBN AISs will transition to MLS mode. Some will continue to operate in the dedicated or system high mode because MLS operating systems and/or applications are not available or there is no mission requirement to operate in the MLS mode.

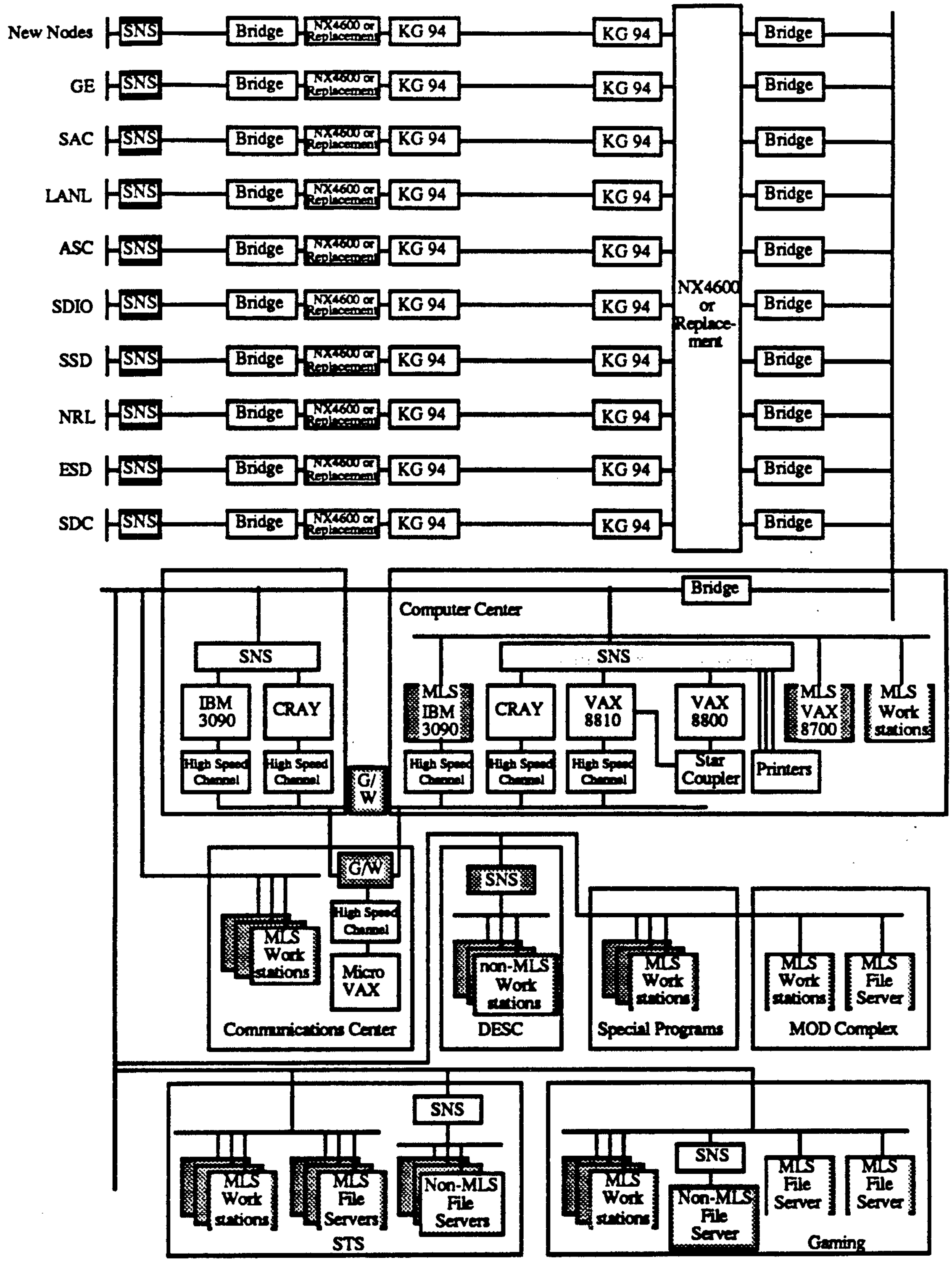


Figure VII-3 Long Term: 1996 and Beyond

ATTACHMENT I

Boeing Secure Network Server and Network Manager Cabilities

Attachment I - Boeing Secure Network Server and Network Manager Capabilities

The Boeing Multilevel Secure Local Area Network (MLS LAN) is a network component providing MLS communication between attached devices. The MLS LAN is composed of multiple Secure Network Servers (SNSs) connected by coaxial cables and a Network Management (NM) workstation. The SNS is a network access device with embedded upper-level DOD protocols, including Internet Protocol (IP), Transmission Control Protocol (TCP), TELNET, and User Datagram Protocol (UDP). The SNS (configured with a video cable plant) also supports analog video transfer through circuit switching capability.

The SNS supports terminal (RS-232C), serial host (RS-232), multiplexed host (IEEE 802.3 or DR-11W), and video (NTSC) subscriber devices, as well as NM and Audit Server interfaces (RS-232 or IEEE 802.3). Terminals are attached to the SNS's terminal device interface card through a standard RS-232C interface. User identification and authentication, access control, and auditing security functions are performed by the terminal device interface card. Hosts are attached to the MLS LAN through either serial (RS-232C) interface cards or host device interface cards. The host interface card supports multiple physical host interface types providing multiplexed services to the host.

The MLS LAN uses a distributed network management approach, with a centralized NM workstation providing system-level monitoring and control, and distributed network management software in the SNSs providing local management support.

The are several upgrades in progress for the SNS and NM workstation. The upgrades will be in evaluation at the A1 level by 1993 (end of near term) and therefore the SNS and NM should be usable at that time. The evaluation phase, normally 18 months long, could be reduced to about 3 months by use of the NSA Scientific Research Center.

The current SNS and NM have some limitations which would affect their use. However, they are being upgraded and these limitations will be overcome with the next versions. The existing problems and solutions are as follows:

(1) The SNS throughput is constrained by the processing speed of the 286 processor. The upgraded versions of the SNS and NM will use 386 processors instead of 286 processors. The throughput and performance should be evaluated in the near term through prototyping.

(2) The SNS throughput is constrained by the SNS-to-NM connection. The NM is responsible for management of Discretionary Access Control data. All audit data is sent to the NM. The NM connects to one of the SNSs using either an RS-232C or ethernet connection. This data path constrains SNS throughput since DAC information is required by the SNS and many actions must be audited before data may be passed. The revised NM will be integrated with an SNS. As a result, the bandwidth will only be limited to the bandwidth of the SNS data bus. This should significantly increase SNS throughput. The throughput and performance should be evaluated in the near term through prototyping.

(3) Currently, each SNS ethernet port can only interface with one AIS. These ports can not be used to process data to/from a LAN with multiple AISs. The upgraded SNSs and NM will provide the capability to allow a connection between an SNS and a LAN which has multiple AISs. This will be accomplished by the addition of IP routing functionality to the SNS and upgrades to the NM to handle the SNS IP changes. This will remove the restriction from using LANs.

(4) The TCP/IP interface to AISs is non-standard. It is a variation of the World Wide Military Command and Control (WWMCCS) host-to-front end protocol. Either an AIS to front end processor or new AIS TCP/IP software would be required to allow an AIS to interface with the SNS as currently designed. The SNS will be revised to use the standard TCP/IP interface. This will enable any AIS with a standard TCP/IP interface to use the SNS. Therefore, the NTF AISs should be able to connect to the SNS without modification.

(5) The NSA evaluation only provides A1 level of trust for Mandatory Access Control (MAC) and Identification and Authentication (I). The NM, which performs Audit (A) and Discretionary Access Control (DAC), is presently being evaluated by NSA at the A1 level. All four elements (MAC, A, I, and DAC) are required for accreditation at the A1 level. When the NSA formal evaluation is complete, the SNS and NM will provide these four elements at the A1 level of trust. Therefore, accreditation at the A1 level of trust should be achievable using SNSs and the NM.

(6) The SNSs communicate with each other as hosts on a "class A" network with an unregistered internet address of "0.x.y.z". This would preclude their use over other networks using IP routing. The upgraded SNS will use "globally assigned ethernet addressing." Therefore, since the upgraded SNS will also use the standard TCP/IP addressing, internetting will be possible. The SNSs do not use the IP security option field for the security label. The upgraded SNS will be use the IP security option field for the security label. Boeing has not developed a secure IP router. However, this functionality will be added to the upgraded SNSs. In the mid or long term, the direct connections between the other NTBN nodes and the NTF may be replaced by DISNET connectivity if links with sufficient trust and bandwidth are available. Correction of these problems will allow the use of SNSs and DISNET connections.

(7) The SNSs (like most MLS devices) require that the trunks connecting them together be "protected", since they do not include encryption. Boeing plans to add type 1 encryption to the SNSs in the future. This will probably take about three years. Type 1 encryption units, such as the NESs, can be used to protect the SNS trunks in the interim. Since the NESs provide centralized key management and other features(e.g., internetting, open architecture), they are a good choice until the SNSs include type 1 encryption.

ATTACHMENT II

Security Engineering Process

Attachment II - Security Engineering Process

In order to achieve the security goal, all aspects of security (computer security, communications security, physical security, and procedural security) must be addressed.

Computer Security (COMPUSEC) will ensure that MLS requirements (e.g., mandatory access controls (MAC), discretionary access controls (DAC), identification and authentication (I&A), and auditing) are addressed. Communications Security (COMSEC) will be ensured by using encryption devices and applying state-of-the-art transmission error checking/data integrity approaches to security and integrity of data. Physical security will address user access to equipment and facilities, user clearances, and TEMPEST controls. Procedural security will ensure that security standards and procedures within the facility are met.

In the past, the development approach of many AISs treated the security functionality and system engineering functionality as separate entities. Due to contractual and budget pressures, the design and development emphasis was placed on system engineering. As a result, security engineering implementation suffered. This approach resulted in a well designed and developed system with a very weak security implementation. Many systems failed accreditation or never became operational due to the lack of security functionality.

The design and development approach for the evolution of the NTBN and NTB nodes must integrate security engineering and system engineering from the beginning. All design and development efforts will incorporate both security engineering and systems engineering requirements throughout the life-cycle of the MLS Network. The result will be an MLS Network that provides the capability for users with various level of clearance to simultaneously access and process data at multiple classification levels.

A. Life Cycle Phases

Six phases of the system life cycle have been identified. The first phase focuses on system requirements analysis. In the second phase, a detailed design is developed. In the third phase, hardware development, software development and unit level testing are performed. In the fourth phase, the Computer Software Component (CSCs) and Configuration Items (CIs) are integrated and tested. The system will be installed and fielded in the fifth phase. The final phase will provide ongoing operations and support.

1. System Requirements Analysis Phase

a. Requirements Definition

During the requirements definition process, the security requirements are identified and analyzed, the Security Policy is defined, and a security model is developed as a high level abstract of the security requirements. Analysis of the requirements and development of the security policy and model are performed in order to produce both an informal and a formal security policy model.

b. Requirements Analysis

DOD 5200.28-STD and the NTB requirements are the key drivers to establishing the final security requirements baseline and the design and development of the MLS Network. The security requirements identified from these sources have been allocated into six major functional areas: Mandatory Access Control (MAC), Discretionary Access Control (DAC),

Individual Identification and Authentication (I&A), Audit, Continuous Protection and Assurance. These six functional areas are the drivers for the development of the security architecture and the test plan.

The System/Segment Specification (SSS), the Philosophy of Protection, and the Security Policy Model are developed together during the System Requirement Analysis phase. The Philosophy of Protection is mapped to the SSS to ensure that the overall security requirements are identified and documented. The Security Policy Model is mapped to the SSS to ensure software design requirements and constraints are identified.

c. Security Policy and Model

The primary source for the Security Policy is the Philosophy of Protection. In addition, other significant sources to the Security Policy are SDI 5206-M, DOD 5200.28-STD, and NCSC-TG-005. The Security Policy presents a mandatory set of rules that are enforced by the security components to support the processing of sensitive data in a secure environment.

d. System Specification

The System Specification defines the system level requirements. The specifications integrate both security engineering requirements and system engineering requirements derived from the requirements analysis described above. These documents further ensure that the security engineering and system engineering requirements and design are integrated to form one complete system, as opposed to establishing separate specification documents which could lead to separate and potentially inconsistent design, development, and implementation results.

2. Design Phase

The preliminary design phase consists of defining a preliminary design for each CSCI and HWCI. Detailed design consists of allocating requirements to Computer Software Units (CSU) and hardware components and establishing design requirements for each unit.

a. Allocation of Policy/Model and Requirements

During the preliminary design, the high level requirement allocations, the security policy, and the security model are decomposed further to begin the detailed system design. Design phase design requirements are established on a component level which is similar to the goal of providing an abstract design of the functions of the Trusted Computing Base (TCB). In the detailed design, requirements are analyzed thoroughly and allocated to the CSCI and HWCI level, CSCIs are broken down into CSCs and CSUs, interfaces are defined, and exceptions and error messages are made. The detailed security design will be incorporated into the overall system design as stated in the System Specification. Although the system will incorporate commercial off-the-shelf (COTS) Trusted Computing Bases (TCB) that have already been evaluated against the Trusted Computer System Evaluation Criteria (TCSEC) requirements, a review of all COTS TCBs will be performed to ensure that all requirements are met by the COTS TCBs' security features. The Detailed Top Level Specification (DTLS), the Formal Top Level Specification (FTLS), and the Software Design Document (SDD) are developed together during both the preliminary and detailed design phases. The detailed design phase is the one point where the approach of two separate development paths for security engineering and system engineering

often cross. Ensuring continued integration of security and system engineering increases assurance that a well designed and secure MLS Network is developed.

b. Documentation

During the design phase, the following documents will be produced: System/Segment Design Document (SSDD), Software Design Document (SDD), Interface Design Document (IDD), Interface Control Document (ICD), and Security Design documentation. The SSDD identifies the security requirements and their allocation to HWCIs and CSCIs. The SDD describes the complete design of each CSCI identified in the SSDD. The IDD and ICD define the detailed design for internal and external interfaces. The security design documentation for this phase consists of the Philosophy of Protection, Security Policy model, and DTLS.

3. Development Phase

During the development phase, the primary activity will be software coding and CSU development based on the requirements established during the detailed design phase.

To provide the requisite levels of assurance for software, the development will be performed in a "closed" security environment. All personnel having access to MLS Network will have sufficient clearance to access the network. Configuration control will be implemented to ensure that applications are protected against the introduction of malicious logic prior to and during the operation of applications. Several assurance requirements, such as extensive functional testing, penetration testing and correspondence mapping between the security model and the design will be implemented. One of the primary goals during the development of the MLS Network will be to ensure that when the final code is developed, it can be trusted to reliably enforce the controls and protection mechanisms required to meet DOD and SDI security guidelines.

4. Integration Phase

The integration phase will occur in three subphases. In the first subphase, the Computer System Units (CSUs) of each Computer System Component (CSC) will be integrated to form the CSCs. At this stage, Unit Development Folders (UDFs) will be developed to document all requirements allocated to the CSC. In addition, unit level testing will be performed. All paths of the code will be rigorously tested during unit level testing. In addition, a covert channel analysis will be performed on the design documents and MLS Network implementation.

The second subphase will integrate the CSCs to form Computer System Configuration Items (CSCIs). Formal test procedures will be developed and a Formal Qualification Test (FQT) for each CSCI will be performed. Security testing will begin during the CSCI testing phase and continue throughout the final System and Integration Testing period.

Once all of the CSCIs have been formally tested, the third subphase of System Integration and Testing will begin. Formal system level test procedures will be developed and Formal System Integration and Testing will be performed. The System Integration and Testing will test the functionality and the security requirements that were not tested at the FQT level. Upon completion of the System Integration and Testing, the Software Test Report (STR) will be written to document both the formal security testing and system engineering testing. The

required security documentation (i.e., the Trusted Facility Manual (TFM), the Security Features User's Guide, and the Configuration Management Plan) will be delivered in this phase.

5. Installation and Fielding Phase

The security aspects of installing the MLS Network will consist primarily of physical security controls. Key issues to be addressed in this phase include the design of physical control zones and protected distribution systems, red/black separation, and verification that the physical installation is fully compliant with applicable DOD and SDI standards and does not invalidate the trusted and secure environment.

6. Operations and Support Phase

Once the MLS Network has been installed, the System Security Officer (SSO) will be required to maintain site security controls. For example, the SSO will add new users and establish access authorizations. In addition, general operations support will be provided to maintain the integrity of the network. Activities during this phase will include training, upgrades, and configuration management. In addition, periodic audit trails will be produced and reviewed and periodic security tests and diagnostics will be performed.

B. TCSEC Development Paradigm

The TCSEC does not explicitly describe a framework for the system development process but does implicitly embody certain design principles. The TCSEC is intended as an evaluation criteria oriented towards the evaluation of the design, instead of the process used in the design. However, in order to achieve a design that can be evaluated at the B2 and higher levels of the TCSEC, it is necessary to follow an implicit design paradigm which consists of developing the following design documentation and correspondence.

1. Philosophy of Protection

Intended to capture the essential security requirements (e.g., access control) and how they are translated into the TCB. This is an informal document which is used to identify the specific TCB protection mechanisms.

2. Security Policy Model

Once the essential security requirements and corresponding protection mechanisms have been identified, a formal model of the security policy can be developed. The formal model is a mathematically precise statement of the security policy for the system under development. Formal models such as the Bell and La Padula Model are often stated in terms of an abstract model and a concrete model. The abstract model captures the essential security requirements while the concrete model provides an abstract set of rules of operation.

3. Descriptive Top-Level Specifications (DTLS)

The abstract rules of operation can then be elaborated into a high-level design specification in the form of a DTLS. The TCSEC defines a Top-Level Specification as "a non-procedural description of system behavior at the most abstract level. Typically, a functional specification that omits all implementation details." The DTLS is written in an informal language and must completely and accurately specify the TCB interface in terms of exceptions, error messages, and effects. The DTLS is intended to capture the user visible actions of the TCB.

4. Formal Top-Level Specifications (FTLS)

The highest level of assurance defined in the TCSEC, A1, requires that an FTLS be developed. The FTLS is written in a formal specification language (e.g., GYPSY) and must be proven to enforce the security policy as described by the formal model. Because most common formal specification languages can not be used to specify temporal properties and subtle hardware characteristics, the FTLS is not required to provide a complete description of the TCB interface. Instead, the FTLS must only provide an accurate description of the TCB interface. Both the FTLS and the DTLS are required in order to fully specify the system under development.

5. Security Policy Model to FTLS Correspondence

To gain assurance that the design will enforce the Security Policy, the FTLS is shown, through a combination of formal and informal techniques, to be consistent with the formal model.

6. DTLS and FTLS Correspondence to the TCB

Once the design has been shown to be consistent with the security policy it is necessary to establish that the TCB is consistent with the design. This is done informally and requires establishing the correspondence between both the DTLS and the FTLS, and the TCB.

7. Covert Channel Analysis (CCA)

Additional assurance of the MLS Network's security is gained through a CCA. A covert channel is defined by the TCSEC to be "any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy". For TCSEC B-Level evaluations, the CCA is informal and is performed on the design documents and MLS Network implementation. At the A1-Level, formal techniques are used and the CCA is usually performed on the FTLS. The continued existence of identified covert channels must be justified.

8. Functional Testing

Functional Testing is similar to that required by DOD-STD-2167A and is aimed at demonstrating that the specifications have been met.

9. Security Testing

Security Testing, sometimes called Penetration Testing is intended to show that not only does the system do what it is intended to do, but that it does nothing else. In particular, Security Testing attempts to, "uncover all design and implementation flaws that would permit a subject, external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB".[5]

[5]DOD 5200.28-STD

10. Security Specific Documentation

a. Trusted Facility Manual (TFM)

The TFM is addressed to the ADP system administrator and presents cautions about functions and privileges that should be controlled when running a secure facility.

b. Security Features User's Guide

Describes the protection mechanisms provided by the TCB and presents guidelines on their use.

c. Configuration Management Plan

Describes the configuration management procedures used for controlling changes to the security components and the MLS Network during their entire life-cycle.

d. Trusted Distribution Plan

Describes the procedures (e.g., site security acceptance plan) used to ensure that the TCB software, firmware, and hardware updates distributed to a site are identical to the master copies.

ATTACHMENT III

MLS Network Prototyping Plan

Attachment III - MLS Network Prototyping Plan

I. INTRODUCTION

A. Scope

This document presents the detailed prototyping plan for the implementation of a Multilevel Secure (MLS) Network prototype. The prototype effort will evaluate security architectures and MLS components to verify that the SDI mission requirements can be supported in an MLS environment. The schedules, estimated resources, and prototyping methodology to be used in the development of an initial prototype and the phased enhancements to the initial prototype necessary to support the implementation and migration from the near term to the long term capability are provided.

B. Objectives

The objective of this document is to define the prototyping effort. It identifies the steps to be performed and describes the procedures to be followed. The plan establishes facility and personnel requirements and specifies the criteria to be used for testing. The relationship between the prototyping effort and operational activities is described. It includes the process of transitioning evaluated hardware, software, and procedures into the operational environment.

II. PROTOTYPING METHODOLOGY

A. Proof of Concept

Rapid prototyping techniques will be used to perform proof of concept and product evaluations prior to implementation of the near term MLS NTF LAN.

The prototyping effort will:

(1) Identify, compare, and select architectures, security components and configurations with the potential of enabling transition to a MLS mode of operation with the recommended levels of trust in the near, mid, and long term.

(2) Determine the degree to which the functional, performance, and security requirements are met by candidate systems which enable MLS operation in various configurations;

(3) Determine the potential effect on operations caused by the use of alternative candidate security components which enable MLS operation in various configurations;

(4) Develop and test the effectiveness of transition strategies designed to progress from a system high and dedicated mode environment to an MLS mode environment;

(5) Devise and test alternative operational, maintenance, and administrative procedures necessary to maintain accreditation;

(6) Confirm the effectiveness of the recommended architecture and security components by performing pre-operational, pre-certification and pre-accreditation trials to ensure the success of operational, certification and accreditation testing.

B. Evaluation Criteria

The prototype will be evaluated against the functional, performance, and security requirements applicable to the near, mid, and long term implementation phases as defined in Section V of the Guidance and Requirements Document.

C. Transition to Operational Mode

Prototype products and procedures that have successfully completed evaluation and verification will be used in the implementation of the operational MLS Network.

III. SCHEDULE

A. Initial Prototype

In order to complete the implementation of the near term capabilities during FY93, the initial prototype must be started NLT (To Be Determined (TBD)) and completed within TBD months.

Based on the current availability of existing MLS security components it is expected that mid term capabilities will be implemented almost concurrently with the development and fielding of the near term MLS NTF LAN. Therefore the initial prototype should also be used to ensure that all mid term requirements will also be met.

The initial prototype effort will consist of the following steps:

(1) Select one, or more, candidate security components and architectures whose characteristics indicate that they have a reasonable potential of satisfying the near and mid term requirements and being usable in the long term timeframes. The selection will be based upon an analysis of the characteristics (functional, performance, and security features) of security components and architectures identified in the Guidance and Requirements Document with the potential to transition the NTF LAN, NTBN, and existing and planned AISs (hosts and workstations) to the MLS mode of operation.

(2) Prepare a plan and procedures for the acquisition of the selected candidate security components and their installation in the prototype environment using the selected architecture.

(3) Acquire sufficient quantities of the selected candidate security components.

(4) Install and instrument (if necessary) the selected candidate security components.

(5) Devise and perform tests and/or develop and run simulations to determine to what extent the candidate security components and architectures satisfy the near, mid and long term requirements.

(6) Evaluate the results of the tests/simulations using the near term requirements as a standard to confirm that the selected security components and architectures support the SDI mission in an MLS environment in the near term.

(7) Evaluate the results of the tests/simulations using the mid term requirements as a standard to confirm that the near term solutions can be transitioned to the mid term environment.

(8) Evaluate the results of the tests/simulations using the long term requirements as a standard to confirm that the near and mid term architectures and security components will support evolution to the long term architectures using the selected security components.

(9) Determine the effect of early (in near term) implementation of mid term requirements (i.e., MLS NTBN).

(10) Provide a recommendation as to the 'most qualified' security components and architectures and the recommended schedule for their implementation.

(11) Develop operational, maintenance, administrative, and security procedures.

(12) Create a plan and procedures for certification and accreditation at the recommended level of trust.

(13) Perform pre-certification and pre-accreditation testing using the prototype configuration.

(14) Support certification and accreditation testing.

(15) Create a plan and procedures for integration of the selected security components into the operational system.

(16) Support the integration of the selected security components into the operational system.

B. <u>Phased Enhancements</u>

Current technology will not fully support "keyboard to database" MLS operations due to the lack of sufficiently trusted (beyond A1) MLS operating systems, applications, and database management systems for the NTB mainframes and workstations. During the mid and long terms, the enhanced prototype will be used as follows:

(1) Evaluate new and emerging MLS products to determine the feasibility of their incorporation into the MLS Network.

(2) Develop operational, maintenance, administrative, and security procedures.

(3) Perform pre-certification and pre-accreditation testing.

(4) Support integration of new and emerging MLS products into the MLS Network.

IV. RESOURCES REQUIRED

A. Manpower

- Initial prototype by Fiscal Year - TBD
- Phased enhancements by Fiscal Year - TBD

B. Equipment/Facilities

- MLS Hardware and Software components
- Use of NTBN and NTB assets for conduct of tests and evaluations
- Facility for prototype staging and evaluation

C. Estimated Costs

- Initial Prototype - TBD
- Phased Enhancements - TBD

V. SUMMARY

Implementation of this plan and commitment of the required resources is required as an initial step to ensure a successful migration path for the NTBN and NTBN Nodes as they transition from the current system high/dedicated mode of operations to a fully accredited MLS Network that supports the achievement of all SDI mission objectives and requirements.

ATTACHMENT IV

NTB Security Strategy Working Group Report

NTB
Security Strategy Working Group

Draft Final Report

March 4, 1991
SDIO/POI

1.0 INTRODUCTION

The National Test Bed (NTB) Security Strategy Working Group (NSSWG) provides this paper for the general use of the NTB community. It is meant to be a living document, and as such, will be updated when deemed necessary by the NSSWG. The current NSSWG members are: the NTB Joint Program Office (NTB/JPO); the NTB Integrating Contractor (NTBIC, the Martin Marietta Corporation); Beta Analytical, Inc. (BAI); the MITRE Corporation; the National Security Agency (NSA); SPARTA, Inc.; and the Strategic Defense Initiative (SDI) Organization (SDIO).

1.1 BACKGROUND

The NTB is a set of distributed, national level assets that support studies, analyses, simulations, gaming exercises, and other scientific activities. Its primary job now is to facilitate the Government's decision making process about developing and deploying the Strategic Defense System's (SDS) elements, as part of the Strategic Defense Initiative (SDI) Organization's (SDIO) mission. The purpose of the NTB is to provide a comprehensive capability to compare, analyze, evaluate and test alternative architectures and key technologies for a strategic defense. Included is the ability to examine technologies in system framework defined by these SDS architectures. The definition and acquisition of this capability has been centralized in order to ensure that a single integrated capability dedicated to the SDI is available to the entire SDI community for addressing the many critical issues necessary to support informed decisions on the future development and deployment of a strategic defense.

The NTB Network (NTBN) can be thought of as a distributed network of heterogeneous systems that support the NTB mission. As Part of that mission, the NTBN must provide an environment that, while providing the requisite security, allows user interaction to the fullest extent possible to nurture the kind of "laboratory setting" that assists in the research process. This laboratory setting can be aided by properly done security.

Each member of the NSSWG has at one time or another proposed a path that, if taken, would provide the NTB with added security. Each has been somewhat successful in some areas, but it became obvious that a consolidated effort, following a single security vision, was needed. It was for this reason that the Director, Information Systems (SDIO/POI) called together the coalition, whose member organizations are identified above, caused it to be chaired by the Assistant Director for Technical Services (SDIO/POIT) and gave it the mission of providing the future vision of security for the NTB. Meetings were held in December 1990 and January 1991 to provide a basis for the needed consensuses and to elicit ideas. This report is based on that effort. Additional meetings will be held in the future to further this activity. This report will be updated as needed.

In recognition of these missions, efforts, and the part that security must play in the proper operation of NTB assets, a guiding policy statement, for the NSSWG, is now given: The NTB shall incorporate security as an *enabling technology* to provide high assurance of information confidentiality and integrity in concert with dynamic resource utilization by a diverse community of users.

1.2 SCOPE

This document addresses the development of a National Test Bed Network Security Architecture. The depth of development is bound by the security perspective. Although operational and user communities were represented on the NSSWG, the primary focus was security. This provided a unique perspective to develop a robust security model. The model enables the NTBN to flexibly reconfigure, meeting user requirements in a secure manner.

This document is not meant to be an in depth analysis of the security needs of the NTBN nor to fully explore all the options available to address those needs. It is rather to identify a method for establishing possible solutions to the perceived need for additional security, in context of the NTB mission as it is understood currently. Example solutions are included to stimulate community-wide discussion.

1.3 REQUIREMENTS

The requirements identified here are with respect to the generalized system and are given as a vehicle for discussing the security requirements of the system.

1.3.1 User Requirements

The NTB must provide users with the computer processing power that will enable them to simulate and validate SDS architectures and designs. This includes supercomputing, workstation graphics, and high speed connectivity among NTB nodes in order for users to accomplish their tasks. It is also includes large amounts of (classified) multilevel information to process; different supporting contractors; and participation, in support of SDI, by Allied scientist. Users with large system simulations will require great amounts of time on supercomputing systems and must have the ability to move the resulting data to various graphic workstations (potentially at various, geographically separated sites) in almost real-time. The roles of different nodes of the NTB will not be addressed here now. Instead, the focus will be upon fully shared resources, the NTF and NTBN. Generally speaking, in support of the above requirements,the NTF must fulfill three major areas of functional requirements. It must act as:

1) Data Center,

2) Test Bed, and

3) Information Resource.

It must fulfill the three major areas in light of: 1) multiple levels of classified data; 2) multiple supporting contractors; and 3) participation of Allied scientific representation.

Again generally speaking, the NTBN must act as the high-speed, wide-bandwidth communications media that would provide the "near real-time" site interactions. Even with just these high level descriptive requirements, we have set the stage for system level security requirements.

1.3.2 System Functionality

In support of the SDI mission, the NTB goals, primarily focused at the NTF, are:

1) To provide a common test environment for the design of SDS.

2) To simulate and validate SDS elements and overall system concepts.

3) To support the planning and conduction of system element and overall system studies and analyses that are excursions to the baseline SDS concept.

4) To provide support to USSPACECOM for Concepts of Operations (CONOPS) and operational training.

5) To serve as a coordination center for SDI field experiments involving multiple ranges and assets.

6) To establish and maintain a state-of-the-art simulation and analysis capability including connectivity to other nodes of the NTB and SDIO Data Centers.

7) To provide a data repository for all SDIO approved software models, system level experiments, and simulation data.

8) To maintain configuration control of all SDS models and SDS operational software.

9) To collect, store, and manage the configuration of standard SDI threat data and generate threat tapes for dissemination to authorized users.

1.3.3 Security Requirements

The NTB must prevent disclosure of classified data to uncleared users and ensure that unauthorized users do not access the system. (This is a requirement on all entities that handle or process classified information, not just the NTB.) To restrict classified data to only those users who are appropriately cleared, the NTB must provide separate processing environments for each level of classified information being processed. Currently, the NTB can support data processing at the unclassified, Secret Collateral, and Top Secret levels. This is in totally separate environments, with no electronic means for the transference of data, nor the capability to process at any adjacent levels (i.e., Secret-only processing). To meet the projected user requirements and to enhance the current capabilities, the NTB, and in particular the NTF and the NTBN should support a Multilevel Secure (MLS) mode of operation (see Section "Multilevel Security"). Also, as more network connections are made and the number of users of the NTB increases, the potential for loss from fraudulent use increases. To prevent this, the NTB must ensure that all users that access the system are authorized to do so. Positive user identification and authentication is required. Therefore, the NTB should investigate other authentication techniques to augment the current password mechanisms (see Section "I&A Beyond Passwords").

2.0 DEFINITIONS & CONCEPTS

2.1 WORKING DEFINITIONS

To provide the NSSWG a good foundation, and to encourage the consistent presentation of ideas, certain generally used terms were given strict definitions. These definitions have help the group focus on the problems at hand (rather than focusing on a particular person's definition of a term). The definitions have also served as a vehicle by which some underlying concerns could be more readily surfaced and dealt with. They are present here for those same purposes. Remember that the focus in on Automated Information Systems (AIS).

1) National Test Best (NTB)
   The AIS equipment, and its environment, that is used to support the SDIO research and development (R&D) effort. The assets may be connected to the National Test Bed Network (which is part of the NTB).

2) NTB Network (NTBN)
   The communication and control media that permits connection between NTB AIS assets. (It Can also be thought of as being bounded by the last electronic connection of any NTB AIS that can communicate with other NTB AISs.

3) NTBN Node
   The AIS equipment, and its environment, at a particular physical location that is used to support the NTB and is connected to the NTBN. (E.g., the NTF or SDC).

4) National Test Facility (NTF)
   The AIS equipment, and its environment, at Falcon Air Force Base, that is used to support the NTB. (E.g., Computer Room 1 and Directed Energy Support Center.) They are connected to the NTBN. (The NTF currently acts as the hub for NTBN communications.)

2.2 SECURITY DEFINITIONS

The definitions were drawn from the, so called, Rainbow Series of documents published by the National Computer Security Center (please see reference section for exact titles) and the Merriam Webster's New Collegiate Dictionary.

1) Audit
   To conduct the independent review and examination of system records and activities.

2) Audit Trail
   A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions froward to related records and reports, and/or backwards from records and reports to their component source transactions.

3) Authentication

1) To establish the validity of a claimed identity. 2) To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.

4) Data Integrity
   1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. 2) The property that data has not been exposed to accidental or malicious alteration or destruction.

5) Discretionary Access Control (DAC)
   A means of restricting access to assets based on the identity of system users and/or groups to which they belong. The controls are discretionary in the sense that a user with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other user (unless restrained by mandatory access control).

6) Identification
   A means of establishing an AIS users identity (generally, a link between user's computer account name and the actual identity of the person(s) authorized use of the account).

7) Identification and Authentication (I&A)
   A means of linking Identification and Authentication methods together to act as a single, security-relevant entity (such as computer logon sequence that requires user's computer identification and password to be given prior to providing any services).

8) Mandatory Access Control (MAC)
   A means of restricting access to assets based on the sensitivity (as represented by a label) of the asset and the formal authorization (i.e., clearance) of users to access information of such sensitivity.

9) Privacy
   1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. 2) The right to insist on adequate security of, and to define authorized users of, information or systems.

10) Protection
   The means, methods and mechanisms used by a system (AIS in this case) to reduce or eliminate access to itself or its resources by some outside force (usually defined as an unauthorized force).

2.3 CONCEPTS OF SECURITY

These concepts of security are included here for background information and to assist in understanding some of the fine points of security, as they may apply to the NTB.

2.3.1 Integrity

The concept of integrity, as here addressed, means that part of an AIS design and/or implementation that concerns itself with protecting information in the AIS from alteration or destruction by an agent or accident. This area is naturally addressed as part of security because the security of an AIS relies, at least in part, on proper labelling of information and

non-contamination of information. Integrity as used here, however, goes beyond what might seem as the natural security concerns. It also addresses issues such as the believability of information derived from computations, consistency of data bases, correct information transfers across networks, and protection of all system information from corruptions. The Trusted Network Interpretation (of the Trusted Computer Security Evaluation Criteria, or TCSEC) (TNI) suggests that along with a Secrecy Policy, some systems will need an Integrity Policy. The NTB is certainly one of those systems.

2.3.2 I&A Beyond Passwords

Password-based authentication systems are vulnerable to a variety of attacks during the life of the passwords such as those associated with the password distribution, selection, duration, and length. Exploiting the vulnerabilities in the password system can result in unauthorized system access. The user identification and authentication (I&A) system for the NTB should be in addition to, or a replacement for the standard password mechanism afforded by most existing operating systems. Passwords themselves are open to several known flaws (e.g., being written down, being easily guessed, wire-tapping). A system that either replaces passwords, or augments them can strengthen user authentication and identification. Alternative A&I techniques could range from biometric systems, to *dumb* cards, to *smart* cards, to cryptographic *challenge/reply* systems.

There are existing biometric systems that perform retina scans of the inner eye, scan thumb prints, or perform combinations of various biometric analyses. *Dumb* cards contain user identity information encoded in a magnetic stripe. The most common form of this card si the commercial credit or automated teller machine card. *Smart* cards are devices that resemble ordinary credit cards, but in fact, contain a microprocessor and memory. The smart card can implement an authentication function (via encryption algorithm) that can positively identify the holder of the card. In a *challenge/reply* system, the user is issued a calculator-like device that is cryptographically unique. A host computer system issues a challenge, based on the user's claimed identity. The user inputs the challenge into the calculator-like device, and then types a reply, generated by the device, back to the challenging system.

2.3.3 Risk Assessment And Two Methodologies

No security system is perfect (nor should any system be considered perfect). The risk that remains in a, proposed, system must be assessed and found to be acceptable, by some authority, prior to processing any classified information on that system. The system's Designated Approving Authority (DAA) should have enough information about the residual risk to make a knowledgeable decision as to whether the system should be authorized to operate or not. Risk assessment methods are also used by system designers so that they do not, accidentally, build systems with insufficient security. There are several different risk assessment methods and several different ways in which their outcome is presented. The two methods briefly discussed here both provide a "risk index." The two methods may come out with different results (indices), but use the same scale and so can be compared. This risk index provides a quantitative measure of the relative "trustworthiness" of a particular system.

There exists two primary methods for determining a computer system's risk index. One method is defined by the National Computer Security Center's "Guidance for Applying the Department of Defense Trusted Computer Systems Evaluation Criteria in Specific Environments" (aka the "Yellow Book"). The other method was defined in a Navel Research Laboratory paper entitled "An Approach to Determining Computer Security Requirements for Navy Systems" Carl Landwehr and H. O. Lubbes. The two approaches differ in that the "Yellow Book" takes a high level view of the system risk (e.g., minimum

level of user clearance versus highest level data processed) whereas the NRL paper includes several more fine detailed aspects of system processing.

The NRL methodology encompasses all of the Yellow Book's methodology, but because of its more fine grained granularity, is ultimately more applicable for use in the NTB environment. The NRL methodology takes into account various types of system users (e.g., programmers versus application users), and their method of communications with the system (e.g., read-only terminal, dumb terminal, smart (programmable) terminal, interactive connectivity, batch connectivity). This provides a more in depth risk analysis and could result in a less stringent set of security requirements based on the environmental usage of the system.

To the greatest extent possible, the NRL method should be used. Situations that make the exact level of vulnerability unclear, should either be further clarified or the, more strict, "Yellow Book" interpretation should be used.

2.3.4 Communities of Interest (COI)

Based on the capabilities and intended use of NTB assets, there will be many NTB users with varying clearance levels and affiliations. The NTB can accommodate these users by partitioning its assets into segments that are appropriate for subgroups of users. These subgroups are referred to as Communities of Interest (COI). A COI can be defined by three entities:

1) A group of NTB users with common access characteristics

2) A set of NTB hardware assets

3) A collection of software and data

Examples of COIs would include the following:

NTB software development teams (One COI for each contracting firm)
NTB/JPO administrators
Experiments (If isolation from general community is desired)
Exercise Participants (One COI for each side to aid in separation)

Defining COIs will be the joint responsibility of the accessing organization and the NTB system's administrator (with input from security). Whatever the basis for the COI, whether it be a common project, sub-project, or function, the list of individuals will be checked for appropriate clearance and need-to-know for the aggregate of information to be available to the COI. Each COI member will have access to all assets allocated to the COI by a combination of physical access controls on the NTB assets and user privileges granted by the NTB Administrator.

2.3.5 Partitioning

The general concept of partitioning is the separation of information, based on some criteria. (I.e., DoD Classification of information) Whether the separation is done electrically, electronically, or in software, all are considered "partitioning." Here, it will mean the separation of information, by appropriate means, over the range of classification of information authorized for a particular Automated Information System (AIS).

In Partitioned Mode, all system users must be cleared to a "High Water Mark" classification level (for the NTB, Secret), but not all would necessarily be authorized access to all compartments on the system. This removes some constraints on system interactions

between different sites (nodes, for the NTBN) by only requiring authorization to those compartments that are needed, rather than authorization to all compartments(as would be necessary in Dedicated Mode). For example, a Partitioned Mode NTBN would allow users who are not formally authorized for both CNWDI and WNINTEL data to use the NTBN (within the confines of the appropriate security policy). This mode will also support additional compartments, as required, without affecting existing users.

2.3.6 Multilevel Secure (MLS)

One can have a system that processes multiple levels of classified information, but not try to "keep it straight" in software (i.e., partitioning). But, in order to process multiple classifications of information (e.g., Top Secret through Confidential), simultaneously, without requiring all users to be cleared to the highest level of data being processed, a Multilevel Secure (MLS) system is required. MLS systems entail security functionality such as mandatory and discretionary access controls (MAC/DAC), audit, and I&A. Associated with the required MLS functionality is the assurance that the MLS mechanisms are designed and implemented correctly. The measure of security functionality and design correctness results in a security evaluation rating as described in the TCSEC and the TNI, among other places.

2.3.7 Provision of Service

Provision of Service, or system availability, is the dual of protection against denial of service. Denial of Service is defined as the means by which a system user, or a process acting on behalf of a system user, can slow down or shut down a system, thereby denying system services to all other system users. Provision of Service can be defined as the set of mechanisms used to prevent Denial of Service attacks. Denial of Service is a threat to both networked systems as well as stand-alone systems but has a far more reaching effect in a networked environment. This is due to scaling factors - users of the network have many systems available for use. Those systems contain a great deal of data - much more so than would be available on a single stand-alone system. Therefore, when service is denied to the network, many more users, systems, and amounts of data are negatively effected. In a network, there is a greater threat of a denial of service attack because of the addition of ubiquitous communications services. In addition to denying service to individual computer systems, the threat exists to deny communication services between computer systems.

2.3.8 System Models For Security

As can be seen in Figure 2-1, Conceptual Secure Component, conceptually it is simple to secure something. Application to a particular component of an Automated Information System will not, in practice, be so straight forward. The general case, however, provides the basis for understanding how this concept would work in the specific case and thus is a good place to start.

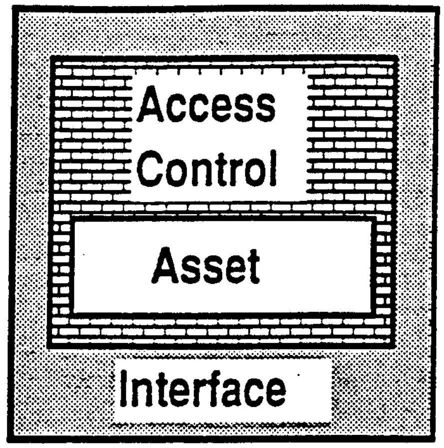


Figure 2-1, Conceptual Secure Component

The generic box identified as INTERFACE is meant to provide a placeholder for whatever it takes to "get to" a particular ASSET. The ACCESS CONTROL represents whatever security measures have been included to protect the ASSET, Limit access to it and control the way in which the world interacts with it. Examples of INTERFACES, ASSETS and their ACCESS CONTROL would include:

INTERFACE	ACCESS CONTROL	ASSET
Door to a room	Lock on door	Personal computer
Log-on routine	Password and I&A	Stand-alone computer
LAN protocols	Label put on by LAN	Network of computers

These few examples are given to provide a basis for understanding. The following sections will provide additional detail. Below is a list of access control features that may be present in one or more of the access control areas:

- MAC Policy Enforcement
- DAC Policy Enforcement
- Separation Policy Enforcement
- Isolation Policy Enforcement
- Privacy Policy Enforcement
- Audit Policy Enforcement
- I&A Policy Enforcement

Figure 2-2, System Element Roadmap, is a stick-figure of a system that has all the elements we are interested in, namely: Hosts (computers),; LANs; WANs; and Nodes (collections of Hosts and LANs, possibly, connected by WANs). Figure 2-3, Element Roadmaps, gives a decoupled view of each of the parts. The Node element will be used in most of the following subsections as our "map" of the system to aid in understanding just where we are.

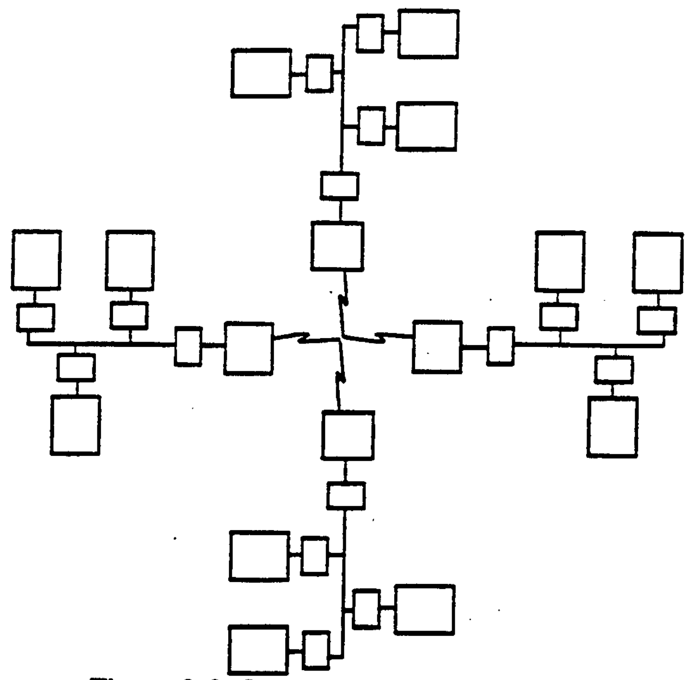


Figure 2-2, System Element Roadmap

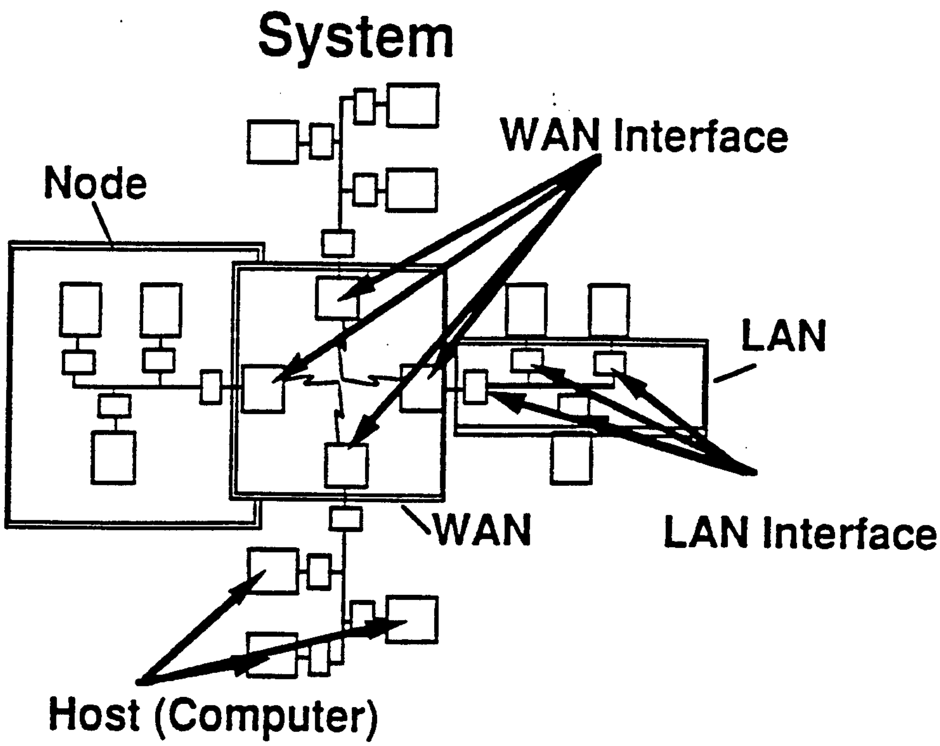


Figure 2-3, Element Roadmaps

2.3.8.1 Hosts

From Figure 2-4, Secure Host Example, the representation of the host may seem overly simplistic (considering the average complexity of most computers and their hardware and software environments). This was done purposefully to provide focus. The

simple model in the figure must be applied to the computer and to each hardware or software component of it separately. For example, there will be word processors that manipulate text in files. The interface to the file is the set of commands initiated by the user and conducted by the word processor. The access control mechanism could be in three parts. The first part could be that within the word processor, itself (if it were properly written). It would check the user's privileges to make the requested changes. The second part would be the Operating System. It would check to see if the user (not the word processor) is permitted to make the requested changes. The third part might be the Information storage system, itself (secure file manager or DBMS). It might check the user's privileges to make the requested changes. At least the second would be done, in a secure environment.

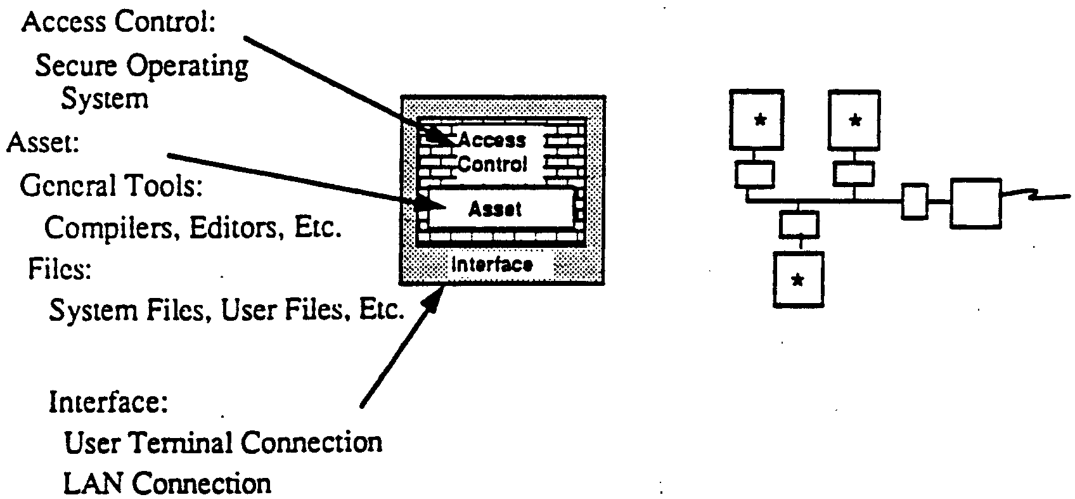


Figure 2-4, Secure Host Example

2.3.8.2 LANs

In Figure 2-5, Secure LAN Example, the network is represented as an "active cable" (i.e., the cable plant and a front end to the network for each asset that must have its own identity, on the network). Good examples of different types of connectivity are: Each host/computer in A Computer Room would have its own front end to the secure LAN, so each computer can be addressed individually (and securely); Single use "LABs" might have a single, "secure front end," so all the assets in the LAB are seen as a single entity, for security purposes; A large lab divided into multiple, smaller work areas, where each small area would have its own secure front end, separate from the others. These represent important decisions where resources (many or few at a time) are seen as a single entity and thus only available to a single group of users at any one time.)

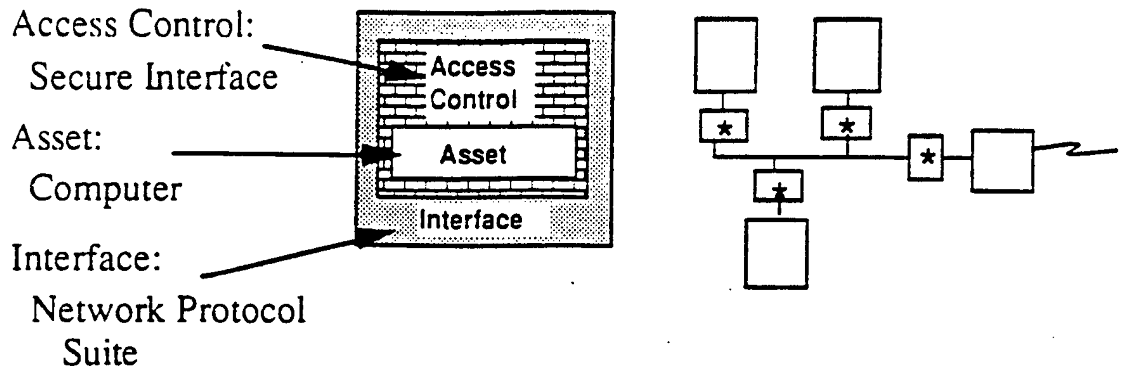


Figure 2-5, Secure LAN Example

2.3.8.3 WANs

In Figure 2-6, Secure WAN Example, the WAN is represented as the communications media between sites that contain hosts and LANs. This is true, but misleadingly simple. The WAN "cable plant" may well represent many interconnected cables (including other WANs and LANs) with tremendous complexity. The simplistic representation here is for three reasons. The first reason for the reduction of any complexity is to provide a vehicle for discussion without getting bogged down in detail, immediately. The second reason to avoid complexity at this level is to permit an "implementation-free" environment to assist in getting all ideas "on-the-table." The third reason is that, regardless of how one makes the WAN, it will be all but transparent to the user (witness the current end-to-end encryption, and each currently proposed replacement that has similar features). The import security features of the secure WAN are the protection of and integrity of the information that transit the WAN.

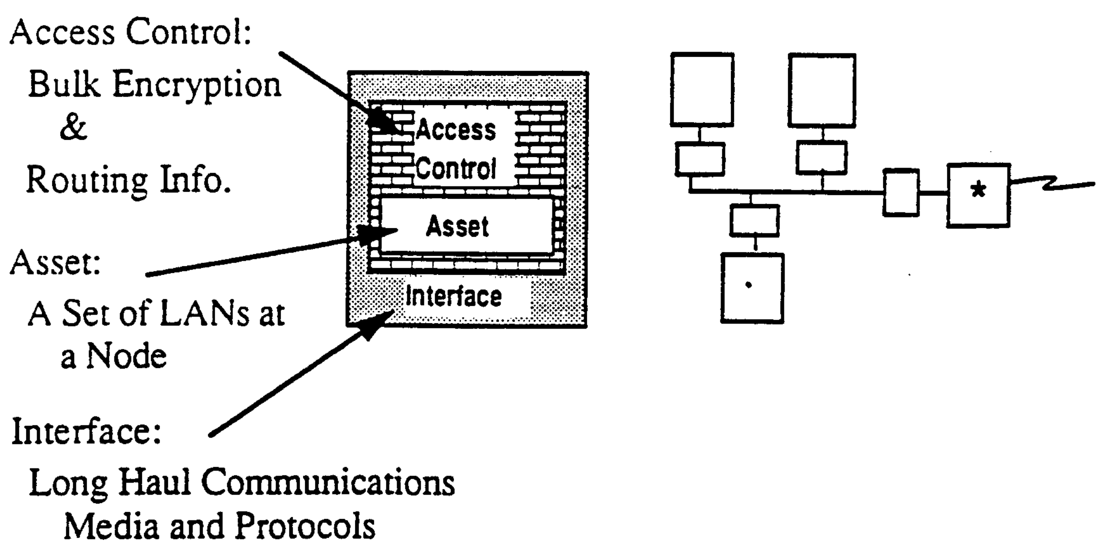


Figure 2-6, Secure WAN Example

2.3.8.4 Systems

Secure systems can be addressed as a sum of their parts. That is, they can be built out of secure hosts, secure LANs and secure WANs. Any additional "glue" between parts general can be placed in one of the above categories. The way one differentiates between a secure system and parts is the paperwork involved. In general, a system will have security policy statements for all security relevant issues to be addressed by any part of the system.

Different parts may address all or some of any part of the system's security policies. A good discussion on the building of secure systems can be found in the Trusted Network Interpretation (TNI, aka Red Book) of the Trusted Computer Security Evaluation Criteria (TCSEC, aka Orange Book).

2.4 SECURITY MANAGEMENT

As can be seen from Figure 2-7, NTB Management, the sphere of influence for the NTB Management encompasses all NTB Member assets, whether connected to the NTBN or not, and the interface to the Customer Community. What is meant by this is that there must be a way of scheduling resources, across the entire NTB, in such a way as to be more efficient in providing services to the greater community of users (in practice, this means that there must be coordination between sites/nodes in scheduling resources and there must be general agreement across all sites/nodes as to the mission of the NTB). The difference between an NTB Member and a Customer of the NTB will be discussed in the next section.

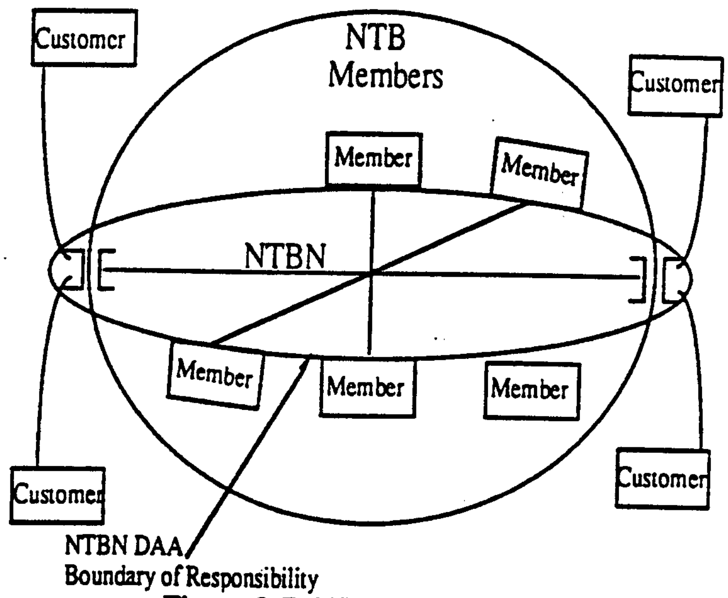


Figure 2-7, NTB Management

2.4.1 Member Vs Customer

The simplest way to delineate between members and customers of the NTB is to say that entities whose funding is provided, to some extent, by SDIO are members of the NTB - all others who wish to use the NTB are considered customers. These simple definitions work well within the security environment, since there is a sense of responsibility to provide security assistance to any entity that is funded by the SDIO, that requests it, and a sense that all others should pay for such service(s), as well as any other NTB resources used.

2.4.2 Memorandum of Agreements (MOAs)

Here we define the MOA as the formal mechanism used to document the, mutually agreed to, connectivity between two NTBN Nodes. In this agreement, security must be addressed to include: level(s) of classified information that ca be exchanged or stored at each facility; level(s) of processing of information at each node; and some agreement as to what labels will be used for the information.

2.4.3 NTF/NTB Coordination Groups

There has been a perception, real or imagined, that the NTB in general, and specifically the NTF are difficult to connect to and use. The NTF Coordination Group (NTFCG, or for now simply NCG) was formed to address these views, at the NTF (and its users) level. The NTB Coordination Group (which has not been formed, yet) will be a NTB-level version of the NTF group, thus serving the entire NTB community.

2.4.3.1 NTF Coordination Group

The NTFCG is the central coordinating group for all initial project requirements definitions and resource forecasts. It coordinates the long- and short-range schedules of all NTF resources and is responsible for recommending and applying scheduling priorities in accordance with NTB/JPO and SDIO policy. A list of all NTF project account numbers vs. contract numbers and/or responsible government agencies is kept to assist in validation of active accounts and projected needs. It also maintains utilization, allocation, and accounting data for all projects at the NTF and provides reports based on that data. In this role, they also will need to be aware of the security implications of proposed, new users as well as the current security status of the NTF.

2.4.3.2 NTB Coordination Group

The NTB Coordination Group will be fashioned after the NTFCG, learning from its mistakes and successes. It will be a team of representatives from each of the sites of the National Test Bed (both NTBN Nodes and sites that are not nodes of the NTBN). NTB-wide resource management issues would be discussed and resolved in this organization.

3.0 METHODOLOGY

The methodology documented in this section is the result of a critical analysis of what has worked (and not worked) in past attempts at applying good system's engineering and analysis techniques to the area of security. It would also seem to apply for any system-widê problem that crosses traditional disciplinary boundaries (unlike software system problems, but like software/hardware integration issues).

The securing of the NTB is, at best, a mammoth task. Critical decisions will be required involving key decision makers. These key decision makers, will not have the time or extensive backgrounds necessary to directly affect an implementable security architecture (and indeed, this is not their role). They do, however, have a responsibility to the NTB community to make the NTB-wide decisions (such as: what constitutes "enough" security; in what security mode will the NTB, as a whole, operate at; and how do the parts of the NTB interact, with respect to security). They, therefore, must find an efficient, cost effective, methodology that will provide them with sufficient information (technical, cost, and schedule) to permit them to make reasonable decisions in a timely fashion. The methodology presented below would support such a process.

3.1 EXPLANATION OF METHODOLOGY

The seven step process identified here sets a course of action that, if followed, will provide the information sufficient so that, along with the consensus of the community, a reasonable decision can be made. It is presented here in a generic form. The next section will tailor it to the solution of the security challenges at the NTB.

- *Step 1: Define Purpose*
  - *Goals to Achieve*

Step 1 provides the focus for the Teams' evaluation. The key decision makers shall set the goals and select the Core Team and the Audit Team. The goals identify the destination. The Core Team will builds the road. The Audit Team provides appropriate technical review.

- *Step 2: Select Core and Audit Teams*
  - *Identify Areas of Required Expertize*
  - *Identify Areas of Engineering Discipline*
  - *Identify User Representation*

The Teams will be selected, by the key decision makers, based on the expertise required by the purpose of the evaluation. Each area must be represented to ensure a high level, wide perspective on the purpose.

- *Step 3: Collect Information*
  - *Establish criteria*
  - *Gather important information from all areas*
    - *Each team member brings a piece of the puzzle*
    - *Any other "parties" that may be concerned are identified*

Step 3 is critical to the success of the evaluation. The Core Team must first agree on the criteria by which potential solutions will be judged. This too will be shaped by the purpose of the evaluation. Early agreement will maintain the focus and keep the Core Team on track. Next each Core Team member researches and brings information from his/her

area. From this information, potential solutions are drawn. The criteria will be screened by the key decision makers and the Audit Team, prior to beginning Step four.

- *Step 4: Evaluate Information Against Criteria*
  - *Models are presented*
  - *User requirements are presented*
  - *Engineering parameters are specified*
  - *Specific Areas capabilities are presented*
  - *Additional considerations are presented*

The evaluation step will begin to identify which proposed solutions are possible. Each area is evaluated and each solution is measured for its ability to withstand repeated attacks.

- *Step 5: Develop Pros and Cons*
  - *Solicit outside review in each area*
  - *Incorporate results of solicitation*

The documentation begins by listing the areas where each solution failed to stand up to the criteria. The Pros and Cons are listed and presented to the Audit Team. This is done to ensure the Core Team did not get "wrapped around the axle" with internal bias. The comments from the Audit Team are noted and the Core Team returns to evaluate for consistence. (consistency)

- *Step 6: Determine Risk of Implementation*
  - *Solicit outside review in each area*
  - *Incorporate results of solicitation*

Since the world of MLS technologies is just evolving, there will be risks associated with each solution. The Core Team will determine those risks based on the criteria, evaluation, pros and cons, and the outside team input. This again will be presented to the Audit Team for another sanity check.

- *Step 7: Report Findings*
  - *Present concrete actions for implementation*
  - *Follow up on (monitor) implementation*

The report ties the whole process back together. Here the solutions are described as how they answer the purpose of the evaluation. They are ranked by the most effective solution to the least. From this report, Senior NTB decision makers will be able to make an informed decision based on a systemic process of evaluating incomplete information.

3.2 IMPLEMENTATION OF METHODOLOGY

It is envisioned that any follow-on effort dealing with securing the NTB will follow the above methodology. Charters for each group should be drawn up from the description of each ones' task(s). The importance of Step 1, Define Purpose, must be stressed. The people putting together the teams (presumably a combination of prospective team members and the key decision makers) should define the purpose prior to any team member assignment or other action on behalf of the team or its effort(s). Once the key decision makers, those responsible for a particular area (or "opportunity" facing the NTB), have been identified/appointed they should set down, in writing, the purpose of the effort they are undertaking. They should also identify the goals of the effort (of course, after seeking technical input for this part, from potential team members). Both the purpose and the goals statements can be revisited during the effort, however, they should not be changed without quit a bit of considered thought, since it on the basis of these statements that the team members were selected.

Once the purpose and the goals statements have been written, the team member choices should be finalized. Each member of each team should bring one or more expertise in areas that are vital to the completion of the teams' tasks. Particular care should be taken in picking the Audit Team members. They will have to "come-up to speed" quickly, when they review the Core Teams' efforts (without a lot of time to do background information gathering). For any follow on to the NSSWG's effort, the following areas must be addressed:

Communications
Operations
Security
Systems Engineering
User Community

The NSSWG has already looked briefly at user requirements that dictate improved system security. However, what is meant by a "criterion" is a, more in depth, look at all the parts of the system and its users. The Core Team (perhaps with assistance from some Audit Team members) will have to "beat-the-bushes" in order to collect a reasonably complete criteria against which to evaluate solutions. This is so because the NTB is an ever-changing set of assets that may or may not have exactly the same mission's statements (each asset can, in fact, have a different focus even when there is a common mission, e.g., one host may be running a threat environment scenario while another emulates a command and control center - they could be working on the same problem, but have completely different needs with respect to security).

Evaluation of a potential solution, against the criteria, is a crucial step in the process. Sufficient information about each proposed solution (in some amount of detail) must be available in order to allow a reasonable evaluation. The following kind of information should be available about each system security solution (as a minimum):

A System Security Model is presented
User requirements are presented
Engineering parameters are specified
Required capabilities are presented
- Communications
- Security
- Operational

Additional considerations are presented
- Communications
- Security
- Operational

In developing pros and cons and evaluating risks, the two teams will have to be careful to keep their roles straight. The difficulty here is expected to be with the Audit Team who, certainly being technically qualified, suggests "solutions" not thought of by the Core Team. Care must be taken in this environment. Either the Core Team and Audit Team must, momentarily "switch places" (with the Core Team now critically analyzing a proposed solution through both the pros and cons step and the risks assessment step) or individual members of the teams must "switch" with respect to this particular point (not advised).

All the steps are vital, however, if Step 7 is not properly done, all the other steps are useless. The reporting of the findings of the teams (not just their conclusions, but how they reached them) should be given as wide as distribution as possible. They will serve to

assist others who may be trying to solve the same kinds of problems and may even apply in other problems within the SDI program.

Although meetings should not be used to simply "get the team(s) together," the NSSWG has found short meetings, or even Video-Teleconferences (VTC), to be very useful. We found that short-fuse tasking, and "quick-looks" at even complicated topics, with reports back to the group (of even intermediate results) helped keep the group focused. The idea of keeping every team member informed and "up-to-date" on any changes is vital so as to not waste the team's time, when meetings are called. (Also, with each member looking at new information *before* meetings, the meetings will be more fruitful).

The NSSWG also found that, if one could draw a picture of a subject under discussion or an idea that was put forth, it was easier to involve the entire team, rather than just talking about a subject. In the next section some of the "strawman architectures" that were developed are presented.

4.0 STRAWMAN ARCHITECTURE

From the discussion on the Conceptual Secure Component, it should now be clear that at any given place in a system architecture, one can identify a security relevant component by describing its task(s)/function(s). Further, to assist in efficient placement of such components, one need only look for potential boundaries between two "groups." Whether these groups are different user groups, with different security/data needs, or these "groups" delineate the difference between an authorized system user and an unauthorized user will assist one in determining what level of precaution (security) on the AIS should apply. To assist in this effort, a policy of the type of security to be enforced at a particular place should be identified/provided. An example of this would be a Mandatory Access Control Policy statement about user's access to assets which could/would be enforced in each path provided the user for connecting to the assets, like on the computers, themselves, the network that connects the user to the computer, or both.

In each architecture picture in the following subsections, an asterisk (*) has been placed at a, potential, security- relevant boundary. In the WAN Figures, connections between sites have asterisks on them, indicating some form of security is required there (currently, bulk encryption is used between connected sites). In the "NTF" Figures, there are several kinds of boundaries indicated by asterisks. On the outside edge of the NTF, there are the boxes with asterisks in them. These boxes represent equipment that must provide the NTF interface to the "outside world." One such set (with "T1" next to them represent one end of the inter-Node connection shown in the WAN Figures (that currently use the bulk encryption). These will be further explained in the following subsections. Implicit in the "T1" box connecting to the interior of the NTF (and PSN) and explicitly in front of the Hosts in Computer Room 1 and in front of the other LABs, there are secure LAN "Front Ends." Whether these are separate boxes of equipment to secure the connection of the assets and protect the information over the cable plant or a board inside a particular computer is irrelevant to this discussion. Only the functionality they provide is important (obviously, this luxury does not extend to the security engineers that will be charged with implementing the "enhanced security" discussed here). We give as a baseline, the following two figures: Figure 4-1, Current WAN and Figure 4-2, Current Node, so that proposed "improvement" measurements may have some common base.

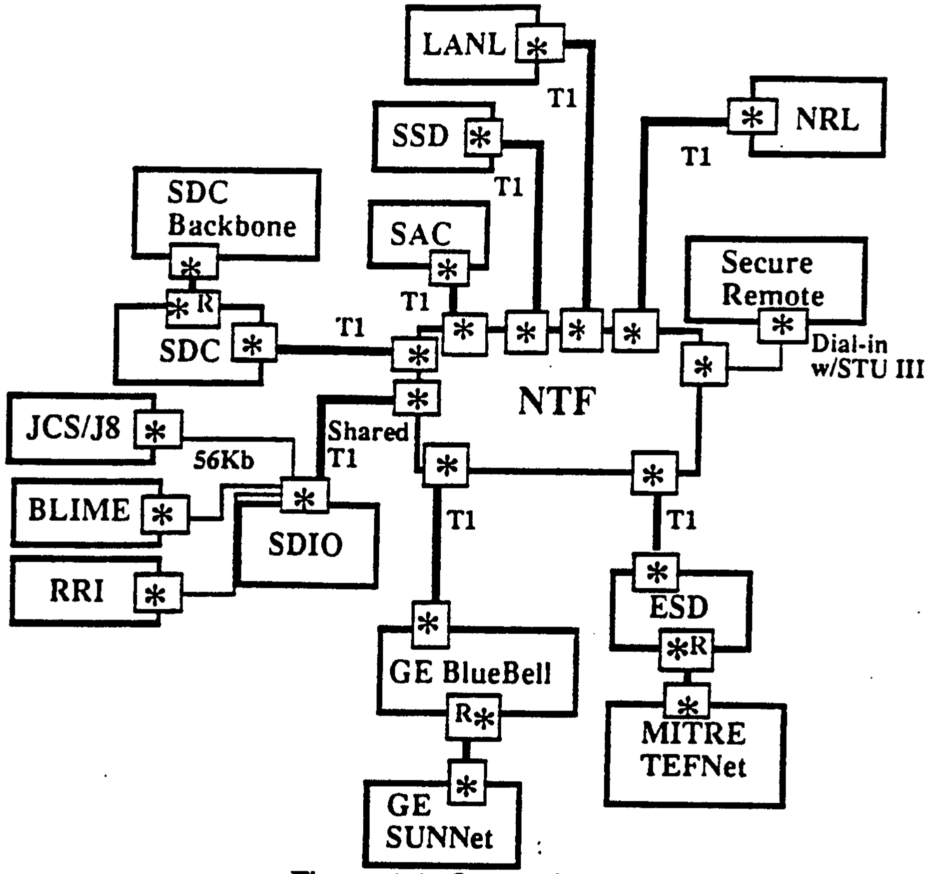


Figure 4-1, Current WAN

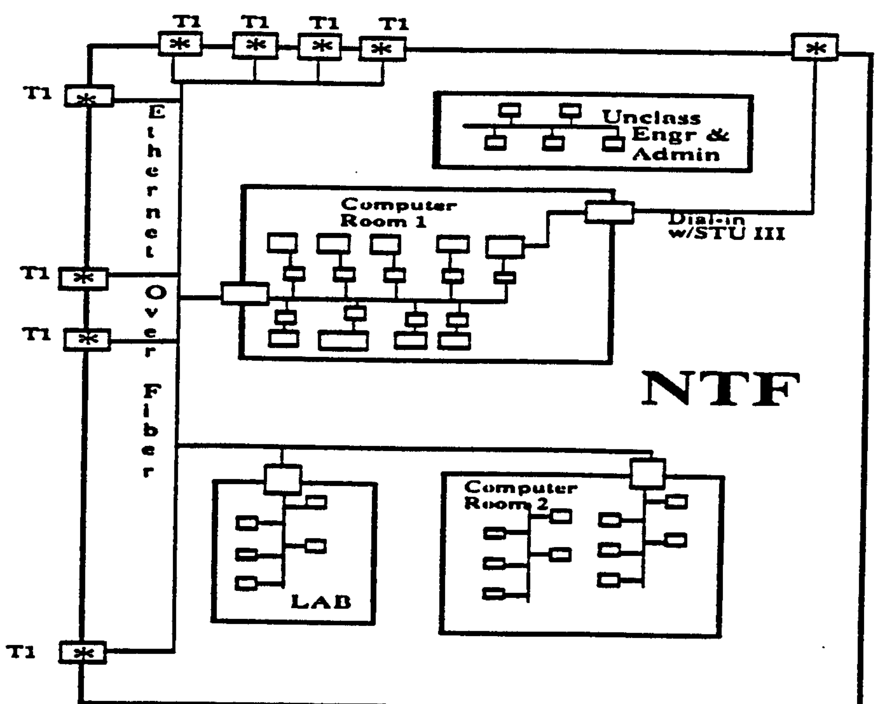


Figure 4-2, Current Node (NTF Used as Example)

4.1 NOW

By "Now" what is meant is those system security capabilities that could be planned and implemented within one to three years that would improve the general security posture of the NTBN and its nodes (using the NTF as a guinea pig). Of particular interest are things that could be done sooner still. For example, the proposed LAN implementation is possible now, using one of several Off-The-Shelf (OTS), NSA approved secure LAN products. In general, however, more planning and analysis is needed before any decision can be made.

The WAN picture, Figure 4-3, WAN Example 2, shows the NTBN with extensions. Note the obvious inclusion of two WANs, represented by DISNET (Secure) and Internet (Unsecure). These are representational - any classified robust, nation-wide communications network could replace DISNET in the figure. The same is true for Internet (any robust, unclassified, nation-wide network could take its place in the figure). The connections, in the figure, to various NTBN Nodes were picked to show all the different kinds of nodes that could be connected and is not meant to be a suggestion list. The communications between NTBN Nodes over the DISNET connection would similar to the current communications with only a few exceptions (albeit important ones). The "back bone" of the current NTBN (see figure Current WAN) is the, cumulative, set of T1 lines, that form dedicated links between the NTF Node and other Nodes of the NTBN. A break down of a single piece of communications gear, anywhere between the NTF and another Node, completely isolates that other node from the rest of the NTBN. With DISNET, even if connection is lost over a particular sub-link, a new path can generally be established. Also, Connection to DISNET, or a similar secure network, requires a Secure WAN front end, like a Blacker device, which supports Type 1 encryption and still provides the routing information required by DISNET's Pack Switched Networks. This gives us the same level of protection on those WAN interfaces that we have now (Type 1 encryption) and yet also provides routing information (not available with our bulk encryptors) that support the multiple routing over the WAN, owned and operated by someone else.

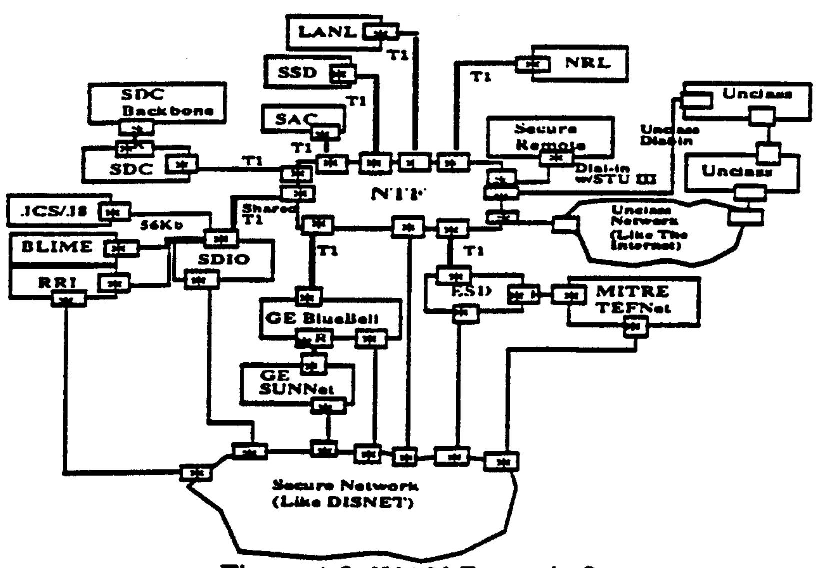


Figure 4-3, WAN Example 2

Even though the connection to the Internet would be operating at the Unclassified level, some form of security (represented by the asterisk on the right hand side of the NTF, in the WAN picture, Figure WAN Example 2), will be implemented to ensure SDI-only,

related unclassified traffic is processed by the system. This will limit the vulnerability of the system from potential abusers while still allowing E-mail and, authorized, remote system log-ons, at the Unclassified level.

On the Node picture, Figure 4-4, Node Example 2, all of the "external lines" coming to the NTF Node, in the WAN picture, are now those lines penetrating the "wall" of the NTF. Note that each box labeled with "T1" has an asterisk. These represent the WAN termination equipment at a node (the NTF, in this case) which would have some security significance (or responsibility). And, note the box labeled "DISNET" has an asterisk in it to remind us that it to is a security relevant boundary. Note, also, the "Dial-In With STU III" box has an asterisk. Obviously, here the STU III is operating in the role of bulk data encryption unit on an non-permanent basis (the connection to the remote site is broken and re-established as needed, unlike the dedicated, full-time "T1" Lines. Also, note the boxes with asterisks at the entrance to "LAB" and "Computer Room 2" and internal to "DESC." These represent LAN security boxes that can separate one lab, or group, from another. Note that the same kind of network box is in front of each asset in Computer Room 1. This obviously indicates that each asset in Computer Room 1 can be in its own group. (If there were only a LAN box in front of the whole computer room {like the case of "LAB"}, all of the assets in Computer Room 1 could only service one group of users at a time, while all other groups would have to wait.) There are also two special purpose boxes in the figures that are identified by function: a gateway/guard (G/G) and a one-way gate (OWG). The names are descriptive of the properties/functions. The G/G acts as a "security guard" at a gate might. It checks traffic going either direction to ensure that the traffic is: 1) permissible; and 2) properly labeled. Traffic that passes the inspection is let through. If some traffic doesn't pass, the G/G reports it and, usually, discards it. As its name implies, the OWG acts like a G/G except traffic is restricted to a single direction.

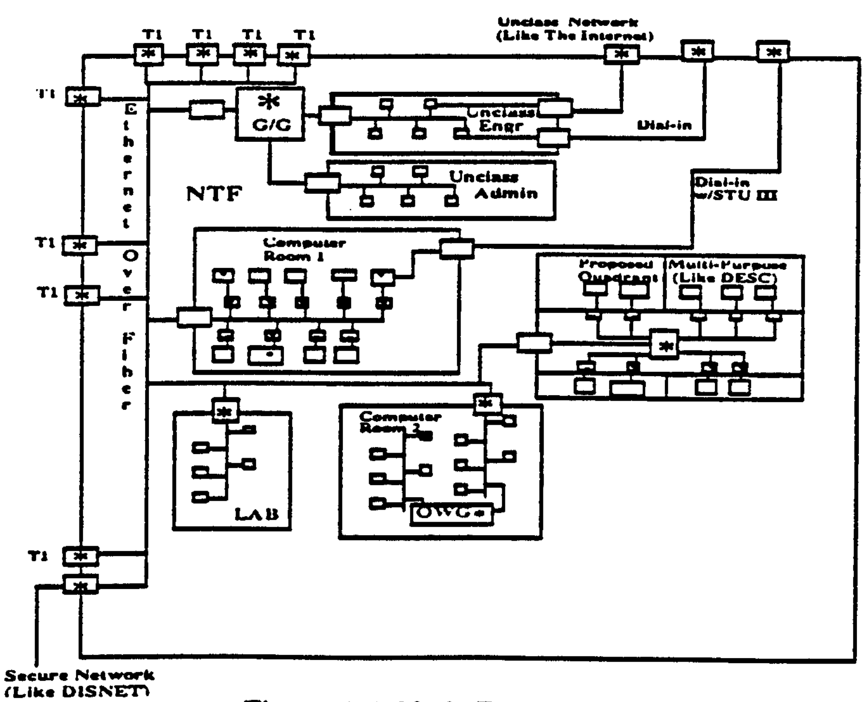


Figure 4-4, Node Example 2

In the next WAN picture, Figure 4-5, WAN Example 3, there are multiple Packet Switched Networks (PSN). Note that the PSN that is noted as being "Located at the NTF" has only a single interface box with an asterisk in it (the box that connects it to the NTF box). The meaning of this will become clear when one looks at the next Node picture,

Figure Node Example 3. There is not other difference between this WAN picture and the last one. However, as will be seen in the Node picture, this one change has both security and operational impacts on the system.

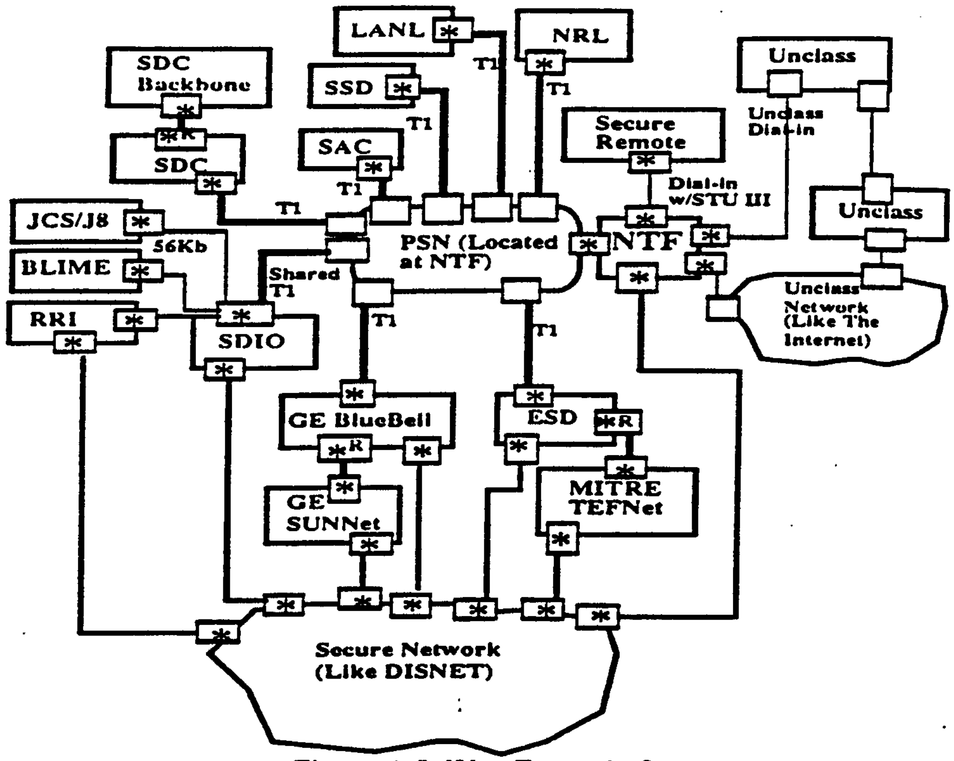


Figure 4-5, Wan Example 3

In the Node picture, Figure 4-6, Node Example 3, we now see that, although the PSN is co-located with the NTF, it is considered "outside" the NTF. The meaning of this is that, for security planning purposes, the entire PSN is outside the security boundary of the NTF (remembering that to have a secure PSN one has to have a secure Front End device, like Blacker that provides the needed routing information as well as the encryption). The other implication is that, now all other nodes of the NTBN can communicate across the PSN without the NTF being in the middle. The plus side is that one is no longer dependent on the NTF being "up" in order to allow nodes of the NTBN to communicate. On the down side, there is now a "choke point" between the NTF and all other NTBN Nodes. That is, now there would only be a, single, T1 speed line going into the NTF from the PSN, which represents its interfaces to all the other NTBN Nodes (before, the NTF connected to most nodes over dedicated, separate T1). These, and any other pluses and minuses would have to weight carefully before any decision could be reached.

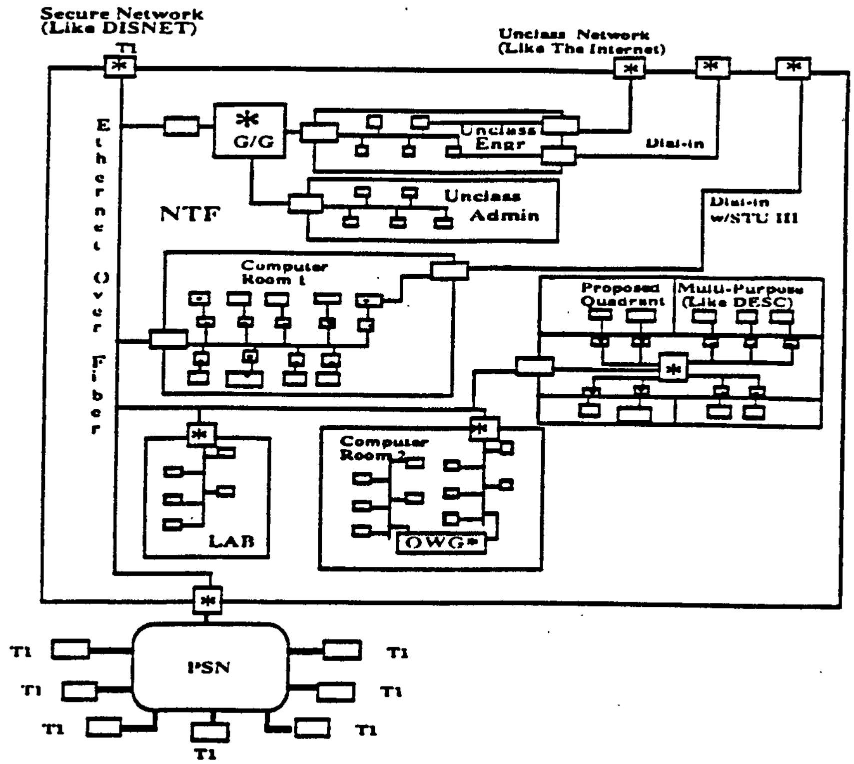


Figure 4-6, Node Example 3

In the Node picture, Figure 4-7, Node Example 4, we extend the PSN "inside the Node" boundary. This alleviates the, so called, choke point from the last discussion, and certainly supplies quite a bit of security (Type 1 encryption between Computer Room 1 and "LAB" for instance). It also, however, brings the limited speed of the PSN into the NTF. The current limit on the Blacker device communication speed is 56Kb/s (Kilobits per second). The suggested speed of the next generation Blacker device is 1.5 Mb/s (Megabits per second) or T1. If the devices were used inside a node, like the NTF, they would be replacing LANs that have speeds on the order of 10 Mb/s. The tremendous slow-down on a nodes internal backbone might not be an acceptable alternative, especially when secure LAN products are available.

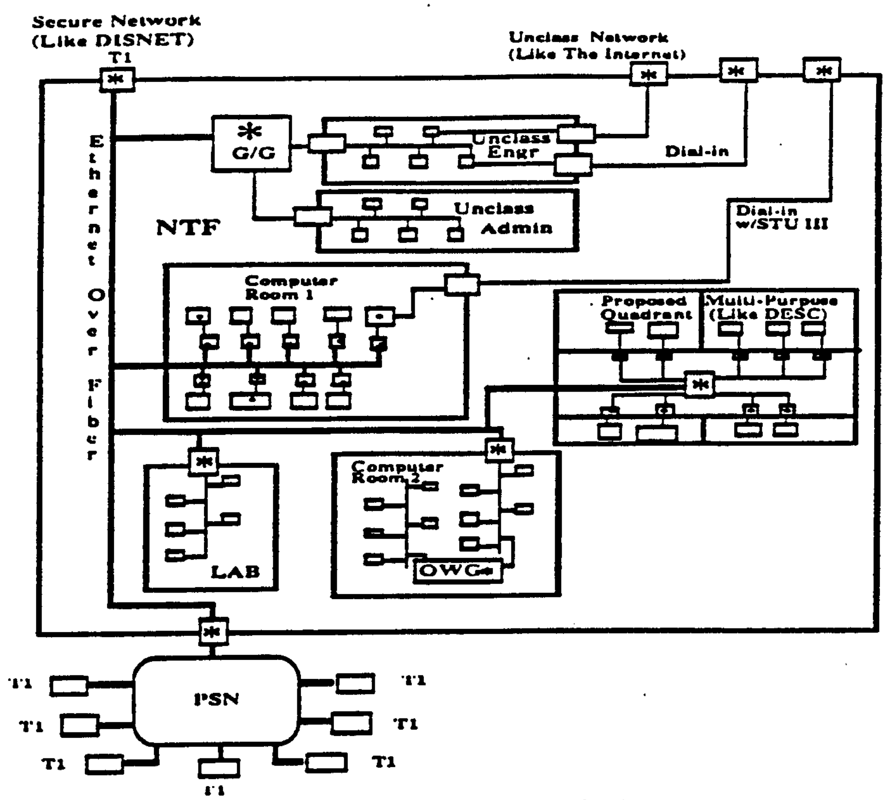


Figure 4-7, Node Example 4

A secure host (computer) was generally not identified (although a couple of hosts in Computer Room 1 were shown with an asterisk in them to denote the presence of some security boundary/feature) in any of the architectural pictures. This in not to suggest that secure operating systems are not currently available (they are, for certain computers). It is rather that the operating systems that do include security feature now, and that have been fully evaluated by the NCSC, are generally not as good as their non-secure counter-parts. This is changing almost daily, so there is reason to believe that the NTBN will be able to have such hosts, but they will be be the exception rather than the rule for several years (where ever secure versions of operating systems are available, it is suggested that they are used to the greatest extent possible, short of making the mission fail by requiring their use). A good first use of a host with a secure operating system would be to allow an unclassified E-mail service, resident in Computer Room 1, but servicing both unclassified LANs and the classified LAN (rules and administrative oversight would have to be established, but this is possible now).

4.1 FUTURE

By future, it is meant here as a system that can be implemented somewhere between five and ten years from now. The architecture can be any of the ones explored in the Now Section, but with the additions of: faster communications media, both on WANs and LANs; secure operating systems for most hosts; and general security "glue" parts, that fill in where some host or network is not security compatible with another like entity.

APPENDIX C

Glossary

I. SECURITY TERMINOLOGY DEFINITIONS

A. Audit

1) To conduct the independent review and examination of system records and activities.

B. Audit Trail

1) A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

C. Authentication

1) To establish the validity of a claimed identify.

2) To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.

D. Data Integrity

1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

2) The property that data has not been exposed to accidental or malicious alteration or destruction.

E. Discretionary Access Control (DAC)

1) A means of restricting access to assets based on the identity of system users and/or groups to which they belong. The controls are discretionary in the sense that a user with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other user (unless restrained by mandatory access control).

F. Identification

1) A means of establishing an AIS users identity (generally, a link between user's computer account name and the actual identity of the person(s) authorized use of the account).

G. Identification and Authentication (I&A)

1) A means of linking Identification and Authentication methods together to act as a single, security-relevant entity (such as computer log-on sequence that requires user's computer identification and password to be given prior to providing any services).

H. Mandatory Access Control (MAC)

1) A means of restricting access to assets based on the sensitivity (as

represented by a label) of the asset and the formal authorization (i.e., clearance) of users to access information of such sensitivity.

I. Privacy

1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information.

2) The right to insist on adequate security of, and to define authorized users of, information or systems.

J. Protection

1) The means, methods and mechanisms used by a system (AIS in this case) to reduce or eliminate access to itself or its resources by some outside force (usually defined as an unauthorized force).

II. SECURITY TERMINOLOGY DEFINITIONS AS APPLIED TO NTB

These concepts of security are included here for background information and to assist in understanding some of the fine points of security, as they may apply to the NTB.

A. Integrity

The concept of integrity, as here addressed, means that part of an AIS design and/or implementation concerns itself with protecting information in the AIS from alteration or destruction by an agent or accident. This area is naturally addressed as part of security because the security of an AIS relies, at least in part, on proper labelling of information and noncontamination of information. Integrity as used here, however, goes beyond what might seem the security concern. It also addresses issues such as the believability of information derived from the computations, consistency of data bases, correct information transfers across networks, and protection of all system information from corruptions. The Trusted Network Interpretation (of the Trusted Computer Security Evaluation Criteria, or TCSEC) (TNI) suggests that along with a Secrecy Policy, some systems will need an Integrity Policy. The NTB is certainly one of those systems.

B. I&A Beyond Passwords

Password-based authentication systems are vulnerable to a variety of attacks during the life of the passwords such as those associated with the password distribution, selection, duration, and length. Exploiting the vulnerabilities in the password system can result in unauthorized system access. The user identification and authentication (I&A) system for the NTB should be in addition to, or a replacement for the standard password mechanism afforded by most existing operation systems. Passwords themselves are open to several known flaws (e.g., being written down, being easily guessed, wire-tapping). A system that either replaces passwords, or augments them can strengthen user authentication and identification. Alternative A&I techniques could range from biometric systems, to dumb cards, to smart cards, to cryptographic challenge/reply systems.

III. MODES OF SECURE OPERATION

A mode of operation in which the Designated Approval Authority (DAA) accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS.

A. Dedicated Security Mode

A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

B. System High Security Mode

A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

C. Partitioned Security Mode

A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode define in DCID No. 1/16, reference (g).

D. Multilevel Security Mode

A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS.

IV. SUMMARY OF EVALUATION CRITERIA CLASSES

The classes of systems recognized under the trusted computer system evaluation criteria are as follows. They are presented in the order of increasing desirability from a computer security point of view.

A. Class (D): Minimal Protection

This class is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

B. Class (C1): Discretionary Security Protection

The trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep others users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

C. Class (C2): Controlled Access Protection

Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through log-in procedures, auditing of security-relevant events, and resource isolation.

D. Class (B1): Labeled Security Protection

Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

E. Class (B2): Structured Protection

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subject and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

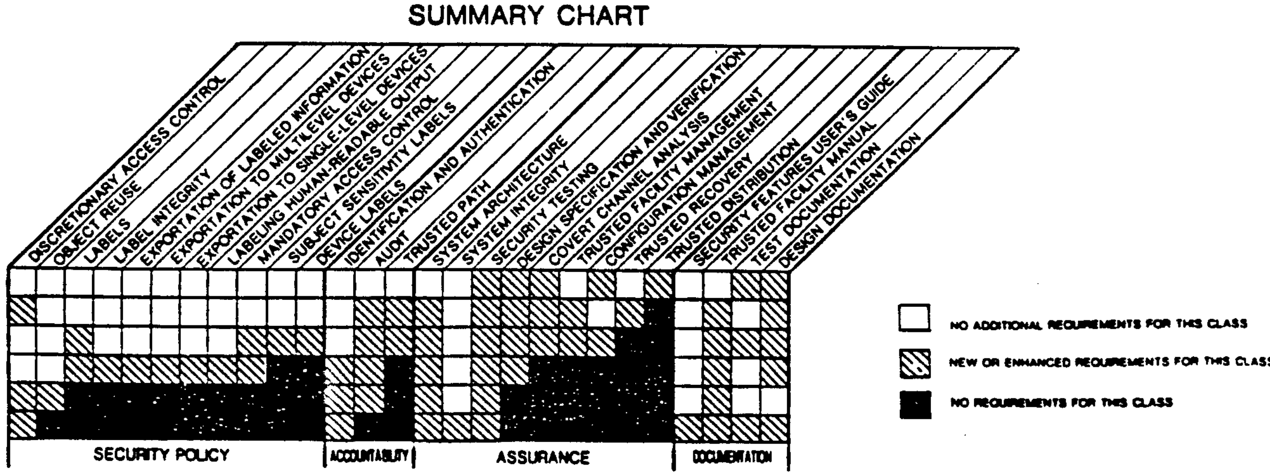
F. Class (B3): Security Domains

The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

G. Class (A1): Verified Design

Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
SUMMARY CHART



ANNEX 1

User Requirements

ANNEX 1

REQUIREMENTS

May 10, 1991

I. INTRODUCTION

The consolidated data in this annex shows a large concentration of NTBN user requirements originating from the Strategic Defense Depute (SD), and a requirement for over 40 T1 communications links. As these data are validated, and as the Theater Mission Defense (TD) user requirements are defined, however, both the size and origin of the NTBN user requirements could change significantly. Thus it is essential that the NTBN have a modular architecture to allow for modular growth.

This annex includes the following appendices:

<u>Appendix</u>

A	Tabulated Requirements Data: This is a consolidated picture of NTB requirements which provides useful insight into the NTBN architecture requirements.
B	NTB User Requirements: This chart shows detailed requirements by user organization, sponsor, sponsor organization, contract code, type, function, user type, node/data rate, and security classification.
C	USASDC User Requirements: This chart shows test concepts/functions by USASDC PMAS participants with their security classification, communications requirements and remarks.
D	SEIC Top Level User Requirements: This appendix includes the detailed surveys developed April 5, 1991 as part of the NTBN effort.
E	Requirements Database Sample: This appendix presents sample user requirements by office (e.g., Locus, Mitre-Arlington).
F	High Level User View: This appendix includes notes developed during the Technology Group organizational meeting held April 9, 1991.

APPENDIX A

Tabulated Requirements Data

CONSOLIDATED REQUIREMENTS AND CONCLUSIONS

The consolidated NTB requirements data provide a very useful picture of NTBN architecture requirements, although complete data were not available for each function and NTF category. Of the 124 NTB User Requirements included, 28 showed planned future requirements, both internal and external. Of the nine SEIC communications requirements identified, four present future needs. There are 31 USASDC requirements, of which nine represent strictly future needs, while five have differing current and future communications requirements. These differing current and future requirements clearly illustrate the need for a flexible NTBN architecture, and reinforce the importance of maintaining the requirements database throughout the evolution of the SDI. The following paragraphs describe the tabulated data which are provided in Tables 1-4. The tabulated data include both current and future requirements.

I. Sponsor Organization

As described in Section IIA, the NTBJPO user data collected by the Requirements Team listed sponsoring organizations under the pre-reorganization of SDIO. For SDIO sponsored functions, the new sponsoring organization was determined through the SDIO Point of Contact (sponsor). It was assumed that the functions followed their SDIO sponsors to new offices, so new office symbols were assigned accordingly. For non-SDIO programs (i.e. programs sponsored by Executing Agents (EAs)), the Team referred back to PMAs via the function, and determined the SDIO sponsor from the PMA. Since the PMAs also still show pre-reorganization office symbols, the SDIO Point of Contact on the PMA was again the key to assigning an SDIO sponsor organization to that function. This latter approach was also used to assign SDIO Sponsor organizations to the SEIC and USASDC data.

Table 1 presents the tabulated data. Out of the 164 functions listed, 101, or 61 percent fall under SD, Deputy for Strategic Defense, and 38, or 23 percent fall under TN, Deputy for Technology. Thus, 86 percent of the identified NTBN test requirements originate from these two deputates.

One can conclude from these statistics that the bulk of current and near-term future requirements for NTBN communications derive from Strategic Defense and Technology programs and in large part from Strategic Defense alone. It is also significant that none of the identified requirements derives from the Global Defense System (SDG). This implies that strategic and technical test requirements are more clearly defined at present than are global (Brilliant Pebbles) and Theater Missile Defense (TMD) test needs. It further indicates that the NTBN architecture must be designed to accommodate these requirements as they develop.

II. User Type

The NTB User Requirements List identifies three user types. Type 1 is Administrative/Data Exchange; Type 2 is Model Development/Batch Simulations; and Type 3 is Interactive, Distributive, or Real-Time Simulations/Experiments. The user type is a critical factor influencing NTBN architecture since it reflects the probable criticality, amount, and duration of traffic.

Functions may involve one or more user type. Neither the SEIC nor the SDC data specified user type, so these were assumed by referring functions back to SDIO PMAs in conjunction with other pertinent information such as user organization. Table 2 shows the breakdown of user type. Of 147 functions, 77, or 52 percent involve both Type 1 and 2, and 32, or 22 percent require all three user types. Thus, the vast majority of NTB users have combined or varying requirements. Well over half of users have no requirement for interactive or real-time

TABLE 1. SPONSOR ORG SORT

SPONSOR ORG.	NTBJPO	SEIC	USASDC PMAs	TOTAL
SDA	38	2	9	49
SDN	8		11	19
SDT	33			33
SD		1		1
TDS	2	1		3
TD	1		3	4
TDI		1		1
TNE	2	3		5
TNS	4		1	5
TNK	5			5
TNI	3			3
TNC	2	1	6	9
TND	10		1	11
POE	4			4
POC	1			1
POI	1			1
AQ	9			9
SIM	1			1
TOTAL				164

TABLE 2. USER TYPE SORT

USER TYPE*	NTBJPO	SEIC	USASDC PMAs	TOTAL
1	17	1	2	20
1 & 2	70	1	6	77
1 & 3	5	2	11	18
1, 2 & 3	17	5	10	32
TOTAL				147
*KEY:				
1 - ADMIN, DATA				
EXCHANGE				
2 - MODEL DEVMT./				
BATCH				
SIMULATIONS				
3 - INTERACTIVE				
DISTRIBUTIVE, OR				
REAL-TIME SIMS/				
EXPERIMENTS				

processing (Type 3). This factor is important to the NTBN architecture because Type 3 users have the most resource intensive requirement.

III. Security Classification

Functional network security classification is obviously critical to the NTBN architecture development. Not all NTB User Requirements functions specified security requirements, however all SEIC and SDC functions identified communications security needs. Table 3 shows the compilation of security requirements. Of the 142 functions identified as having security requirements, 103, or 72 percent required Unclassified to Secret or Secret. Further, 26 functions, or 17 percent, have security requirements beyond the Secret level. These data validate the view that the NTBN architecture must support a Multilevel Secure (MLS) mode of operation.

IV. Data Rate

The data rate requirements were the most difficult to correlate. Table 4a shows the numerical data as available for NTB User and USASDC communications needs. Table 4b shows SEIC communications data types. Of the 79 functions providing numerical requirements, 46, or 58 percent require a data rate of T1. Tables 4a and b illustrate very clearly the wide variation in communications requirements for the NTBN. Taken together with the raw data presented in the appendices, these requirements lead to the conclusion that the data capacities must be flexible as requirements vary from one function to another and also vary between phases of a particular function. Only five dial-up requirements were identified, which indicates that the communications needs are less transient in nature than may have previously been supposed. The raw data also show no correlation between user type and required data rate as might have been expected.

TABLE 3. SECURITY CLASS SORT

HIGHEST SEC. CLASS	NTBJPO	SEIC	USASDC PMAs	TOTAL
UNCLASS PROP.	1			1
UNCLASS	3		8	11
UNCLASS-CONFID	1			1
UNCLASS-SECRET OR SECRET	81		22	103
SECRET & WNINTEL		5		5
SECRET, WNINTEL, +	7	1		8
SECRET/TS/SAR	2			2
SECRET/TS/SAR +		1		1
TS	2	3		5
SECRET & TS/COMSEC		1		1
SECRET, TS/SCI	1			1
SECRET, TS, SAR, SCI		1		1
SECRET, CMWDI	2			2
TOTAL				142

TABLE 4A. COM REQ SORT (ALL DATA, UNLESS OTHERWISE NOTED)				
		USASDC	PMAs	
DATA RATE	NTBJPO	DATA	# DATA/VOICE	TOTAL
9.6 KB/SEC		5	2	5
	0			
19.2 KB/SEC		3		3
56 KB/SEC OR	4	9		13
< 56 KB/SEC				
> 56 KB/SEC		5		5
				0
T1	34	12	2	46
T3		2	1	2
DIAL-UP	5			5
TOTAL				79
		TABLE 4B.		
DATE TYPE	SEIC	# DATA/VOICE		
DOCUMENTATION	2			
IMAGERY	1			
INTERACTIVE	5			
INTERFACE	3			

APPENDIX B

NTF User Requirements

REV 2

User Organization	Sponsor	Sponsor Org	Contract #	Type	Function	User Type	Node/Data Rate	Exp. Security
CURRENT EXTERNAL								
Advanced Technologies	Maj. Bennett	SSD/ALI	F04901-88-D-0026	S	Space Supportability Models (COSEMS)	Type 1,2	SSD-T1	Secret
Analytic Services Corp.	On user support list but not in current user database AQ			S	System Analysis (SODSIM)	Type 1,2	SDIO	
Applied Research - Arlington	James Dryden	SDIO/POE	SDIO-84-88-C-0018	S	Architecture Analysis	Type 1,2	SDIO	
Applied Research - Huntsville	Jimmy Burch	USASDC SDA	DASG-60-86-C-0060	S	Ground Based Supportability (LOGAM)	Type 1,2	SDIO	Secret
Army Missile Command	C. Mikkelsen	AMSMI-RD-SS-AT	Gov't Agency	B	Ground Based Element Development	Type 1	SDC - dial-up	Unclass - Secret
Automation Research Sys.	LTC. Hawthorne	SDIO/ENT	PMA-N2300 (NRL)	S	NRL Support, SDI Test and Evaluation?	Type 1,2	SDC	
BDM Intern'l (Super SETA)	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0017	O	GPALS Studies/User Surveys	No Current Comm Requirement		
Blime, Inc.	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0035	S	SODSIM Development/Sys. Analysis	Contract Expired		
Booz, Allen, & Hamilton	Billy Love	SDIO/POC	SDIO-84-88-C-0019	O	Planning and Control	Type 1	SDIO	
Coleman Research Corp.	Bill Mobley	USASDC SDA	DASG-60-88-0100	B	Ground Based Element Models for Level 2	Type 1,2	NTF, SDC - T1	Secret
Coleman Research Corp.	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0017			Type 1,2		
Colsa, Inc.	Rolland Dace	SDC-CSSD-SA-BB	DASG-60-89-C-0092	T	Mid Course Data Center, ARC Support	Type 1,2	SDC - T1	Secret
Computer Sciences Corp.	Col. Nagy	SDIO/EN SDA	SDIO-84-88-C-0020	S	Sys. Integration & Engineering Support	Type 1,2	GE - T1	Secret
Decision Science Applic.	James Dryden	SDIO/POE	SDIO-84-88-C-0018	S	Effectiveness Models (SODSIM)	Type 1,2	SDIO - dial-up	Secret
Dynamics Research Corp.	Allen Leary	SDIO/ENE	SDIO-84-88-C-0017	S	SDI Supportability Anal. (LOGAM/COSEMS)	Type 1,2	SDIO	Secret
Dynamics Research Corp.			SDIO-84-90-C-0002	O	Technical Information Center?	Type 1,2	SDIO	
ESD/XRS	LTC. Toole	SDIO/TND	Gov't Agency	S	Command & Control/SOIF	Type 1,2,3	ESD - 56 kb-T1	Secret
GE Aerospace - Bluebell	Col. Nagy	SDIO/EN	SDIO-84-88-C-0020	S	SDI Systems Engineer	Type 1,2,3	GE - T1	Secret, WNINTEL +
GE Aerospace - Colo. Springs	Col. Nagy	SDIO/EN	SDIO-84-88-C-0020	S	SDI Systems Engineer	Type 1,2	GE WAN	Secret, WNINTEL +
GE Aerospace - Arlington	Col. Nagy	SDIO/EN	SDIO-84-88-C-0020	S	SDI Systems Engineer	Type 1,2	GE WAN	Secret, WNINTEL +
GE Aerospace - LA	Col. Nagy	SDIO/EN	SDIO-84-88-C-0020	S	SDI Systems Engineer	Type 1,2	GE WAN	Secret, WNINTEL +
General Research Corp. - Huntsv	Joseph Latham	USASDC	DASG-60-88-C-0118	B	Command and Control (ARGUS)	Type 1,3	SDC, >T1 (Future)	Secret
General Research Corp. - Arlington	Capt. Palmer	SDIO/TNS	SDIO-84-89-C-0012	T	NORSE Code (Nuclear Effects Modeling)	No Current Comm Requirement		
Grumman Space Systems Div.		SSD	F04701-87-C-0023	T	Space Power and Propulsion	Type 1,2	SSD	Secret/TS/SAR
Grumman Space Systems Div.		USASDC TND	DASG-60-90-C-0103	T	NPB Experiment Design	Type 1,2	SDC	TS
Grumman Space Systems Div.		USASDC TND	DASG-60-88-C-0025	T	NPB Experiment Design	Type 1,2	SDC	TS
Grumman Space Systems Div.	TNS?	SDIO	SDIO-84-89-C-0005	T	Strategic Early Warning	Type 1,2	SDIO	Secret/TS/SAR
HQ SAC/XRF	Dr. Carlson	SDIO/PT SDA	Gov't Agency	S	Command and Control Gaming	Type 1,3	SAC - T1	Secret
Huntsville Sciences Corp.	LTC. Martin	SDIO/TNK	DASG-60-90-C-0011	T	Aerothermal Analysis	Type 1,2,3	SDC	Secret
Institute for Defense Analysis	LTC. Hochberg	SDIO/ENA SDA	MDA-903-89-C-0003	S	Architecture Studies and Analysis	Type 1,2	SDIO, NTF	Secret
Joint Chiefs of Staff-J8	Capt. Chisholm	USN SDA?	Gov't Agency	S	Threat, Gaming, Architecture Studies	Type 1,2,3	SDIO - 56 kb	Secret, TS/SCI (Fu
Kaman Sciences (Prime)	Dr. Bob Becker	USASDC TNK	DASG-60-90-C-0011	T	Aerothermal Analysis	Type 1,2	NTF	Secret
KDEC	CDR. Korejwo	SDIO/TNS TNC	Gov't Agency	T	Kinetic Energy Digital Emulation Center	Type 1,2	SDC - T1	Secret
Los Alamos National Laborato	Col. Koval	SDIO/PTN SDT	Gov't Agency	T	NPB Models, DETEC Development	Type 1,2	LANL, <T1 rqmt	Secret
Locus, Inc.	Nelson Head	NRL	PMA-N2300 (NRL)	O	NRL Computer/Networking Support	No Current Comm Requirement		
MMC-Liason	Col. Koval	NTBJPO SDT	F19628-88-C-6012	O	Washington Liason	No Current Comm Requirement		
Mission Research - Nashua	LTC. Berggren	DNA TNE	DNA-001-88-C-0078	T	High Altitude Nuclear Environments	Type 1,2	ESD, 56 kb	Secret, CNWDI (Fut
Mission Research - Huntsville	On user support list but not in current user database			T	Nuclear Environments	Type 1,2	SDC - T1	Secret, CNWDI (Fut
Mitre - Arlington	On user support list but not in current user database			O	MITRE SDIO Liason, Long Range Planning	No Current Comm Requirement		
Mitre - Huntsville	Billy Carter	SDC/BMC3	DAA-B07--91-C-N751	T	Common Test Environment (CTE)	Type 1,2	SDC - T1	Secret
Mitre - Bedford	Steven Cote	ESD	F19628-89-C-0001	S	ESD Support, C2/SOIF, CTE	Type 1,2,3	ESD - T1	Secret

SDA (38) SDN (8) TNI (3)
SDT (33) TD (1) INC (8)
INC (2) TND (10)
TNS (4)

REV 2

User Organization	Sponsor	Sponsor Org	Contract #	Type	Function	User Type	Node/Data Rate	Exp. Security
Naval Research Lab.	Nelson Head N2350	NRL SDA	Gov't Agency	S	Comm/Architecture Modelling, Threat	Type 1,2	NRL - T1	Secret
Nichols Research - Huntsville	Bill Mobley	USASDC SDA	DASG-60-88-C-0100	B	Ground Based Element Models for Level 2	Type 1,2	NTF	Secret
Nichols Research	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0017					
Optimization Technology, Inc.	Rolland Dace	USASDC SDN	DASG-60-89-C-0092	T	NTBSIM, ARC Support	Type 1	SDC, <T1 Rqrd	Unclass-Secret
PRC, Inc.	Maj. Bennett	SSD/ALI SDA	F04701-88-D-0028	S	Logistics and Cost Modelling (COSEMS)	Type 1,2	SSD - T1	Secret
Physical Research-Huntsville	Maj. Eric Imker	SDIO/TNS TNS	DNA-001-88-C-0030	T	Nuclear Environments Software	Type 1,2	NTF, SDC - T1	Secret
Physical Research-Huntsville	Dr. D. McClure	USASDC TNK	DASG-60-90-C-0134	T	Aerothermal Research	Type 1,2,3	SDC	Secret
Physical Research Santa Barb.	LTC. Berggren	DNA TNI ?	DNA-001-88-C-0030	T	Nuclear Environments Software	Type 1,2	SSD/LANL - dial-up	Secret
RJO Enterprises	Eloise Brooks	SDIO/EN AQ	SDIO-84-88-C-0052	O	Test and Evaluation Activity Summary	Type 1	SDIO, <T1 Rqrd	Secret
Riverside Res. Inst. (Super SETA)	COL. Richardson	SDIO/TID TD	SDIO-84-88-C-0019	S	Arch./Element Development/Threat	Type 1,2	SDIO, No Longer Rqr	Secret/CNWDI/WNINTEL
R&D Associates	Capt. Shirley	SDIO/TND TND	SDIO-84-87-C-0001	T	Starlab/Directed Energy Research	Account Suspended		
SAIC - Huntsville	Ronald Smith	USASDC SDA	DASG-60-88-C-0066	B	AMEM, Threat, Element Model Dev.	Type 1,2	SDC - T1	Secret
SAIC - Huntsville	Ronald Klasser	USASDC SDA	SDIO-84-88-C-0020	O	SEIC Threat	Type 1,2		
SAIC	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0017	B				
SDIO/EN	Col. Nagy	SDIO/EN SDA	Gov't Agency	O	SDIO Engineering Directorate	Type 1	SDIO	Unclass - Secret
SDIO/POI	Elaine Litman	SDIO/POI POI	Gov't Agency	O	SDIO Information Systems Security	Type 1	SDIO	Unclass - Secret
SDIO/PTN	Col. Koval	SDIO/PTN SDT	Gov't Agency	O	SDIO Management, Sys. Analysis	Type 1,2	SDIO - T1	Secret
SPARTA - McLean	COL. Fletcher	USAF SDA	SDIO-84-88-C-0018	S	Architecture Analysis	Type 1,2	SDIO	Secret
SPARTA - Huntsville	Laurie Fraser	USASDC SDN	DASG-60-88-C-0023	B	Ground-Based Element Development	Type 1,2	SDC	Secret
SPARTA - Huntsville	Francis Cheek	USASDC SDN	DASG-60-88-C-0050	B		Type 1,2	SDC	
SRS Technologies - Arlington		SDIO/POE POE	SDIO-84-89-C-0019	S	MEM, SODSIM Analysis	Type 1,2	SDIO - T1	Secret/NOF/CNWDI/WNIN
SRS Technologies - Arlington	Capt. Kelsey	SDIO/ENT TDE	SDIO-84-89-C-0021	S	SDI Test and Evaluation Support	Type 1	SDIO - T1	Secret/NOF/CNWDI/WNIN
SRS Technologies - Huntsville	Laurie Fraser	USASDC SDN	DASG-60-88-C-0023	B	Ground Based Element Mod. Development	Type 1,2		
SSD/CN (CNIES)		SSD SDA	Gov't Agency	B	Space Based Element Dev., Gaming	Type 1,2,3	SSD - T1	Secret
SSD/XRP	Allen Leary	SDIO/ENE SDA	Gov't Agency	S	Space Based Supportability	Type 1,2	SSD - T1	Secret
Starlab/Directed Energy	Capt. Shirley	SDIO/TND TND	SDIO-84-87-C-0001	T	Analytic Sim. Modelling for DE	Type 1,2,3	NTF,SDIO,ESD,SSD,SDC	Unclass - Secret
System Planning Corp.	Col. Sheldon	SDIO/SIM SIM	MDA-903-86-C-0189	O	SDIO Countermeasures	Type 1,2	SDIO	
TRW	Michael Gately	USASDC SDA	DASG-60-89-C-0157	B	EV Performance Analysis (ARGUS)	Type 1,3	SDC - T1	Secret
Teledyne Brown- Huntsville	CDR. Jenkins	SDIO/ENS SDA	DASG-60-87-C-0042	B	Level II Sim. Dev. (ASAT Modelling)	Type 1,2	SDC - T1	Secret
Teledyne Brown - Huntsville	Jimmy Burch	USASDC SDA	DASG-60-86-C-0080	S	Ground Based Element Supportability	Type 1,2	SDC	Secret
Teledyne Brown- Colo. Spr.	CDR. Jenkins	SDIO/ENS SDA	DASG-60-87-C-0042	B	Studies and Anal./ASAT Modelling/BMC3	Type 1,2	NTF	Secret
Teledyne Brown - Arlington	LTC. Hawthorne	SDIO/ENT TDS	SDIO-84-86-C-0021	S	SDI Test and Evaluation Support			
TASC - Huntsville	Capt. Shirley	SDIO/TND TND	SDIO-84-87-C-0001	T	Starlab/Directed Energy	Type 1,2,3	SDC - T1	Secret
TASC-Arlington (Super SETA)	James Dryden	SDIO/POE POE	SDIO-84-88-C-0018	S	Architecture Analysis (SODSIM)	Type 1,2	SDIO - T1	Secret
USA Strat. Defense Command	Doyce Satterfield	USASDC SDA	Gov't Agency	SBT	Architecture/Elem. Dev./BMC3/Environ.	Type 1,2,3	SDC - T1	Secret
USSPACECOM/J4-J6	LCOL Reznick	USPACECOM SDA	Gov't Agency	O	C2 Gaming/EAC VAX Usage (non-SDIO)	Type 1,3	PAFB	Secret
W. J. Schafer Assoc.	Capt. Shirley	SDIO/TND TND	SDIO-84-90-C-0056	T	Optical Modelling for Laser Control	Type 1,2	dial-up	Secret
W.J. Schafer Assoc.	LCOL. Skvarenina	SDIO/ENA AQ	SDIO-84-88-C-0017					
CURRENT INTERNAL								
ARINC	Nat Sojourner	NTBJPO SDT	SDIO-84-90-C-0028	O	NTBJPO SETA Support	Type 1	NTF	Unclass - Secret
CAE-Link	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	S	Command and Control Gaming	Type 1,2	NTF	Secret
Carnegie Mellon University	Bob McCauley	NTBIC SDT	NTBIC Sub	T	Software Development Standards	Type 1	NTF	Unclass-Secret

 REV 2

User Organization	Sponsor	Sponsor Org	Contract #	Type	Function	User Type	Node/Data Rate	Exp. Security
CTA	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	S	C2 Gaming, System Simulator, Perf. Anal	Type 1,2	NTF	Unclass-Secret
Cray Research	Steve Otsuki SDT	NTBIC Vendor	F19628-88-C-0012	O	NTBIC Vendor	Type 1	NTF	Unclassified
GE	Col. Nagy	SDIO/EN SDA	SDIO-84-88-C-0020	S	SDIO Systems Engineering	Type 1,2	NTF	Secret
Geodynamics	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	S	Studies and Analysis/Org. Conflict of Int.	Type 1,2	NTF	Secret
Hughes	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	O	NTBIC Communications	Type 1,2	NTF	Secret
IBM	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	O	Technical Information System	Type 1	NTF	Unclass-Secret
Logicon	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	S	Threat	Type 1,2	NTF	Secret
Martin Marietta - Info. Sys.	Col. Koval	NTBJPO SDT	F19628-88-C-0012	S	NTB Integration Contractor	Type 1,2,3	NTF	Unclass - Secret
Martin Marietta - Data Sys.	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	O	NTBIC Operations and Maintenance	Type 1	NTF	Unclass-Secret
MITRE - Colorado Springs	Nat Sojourner	NTBJPO SDT	DAAB07-91-C-N751	O	NTBJPO Technical Evaluation	Type 1,2	NTF	Unclass-Secret -
Nicols Research	Steve Otsuki	NTBIC SDT	F19628-88-C-0012	S	System Simulator, Studies and Analysis	Type 1,2	NTF	Secret
NTBJPO Staff	Col. Koval	SDIO/PTN SDT	Gov't Agency	S	NTB Joint Program Office	Type 1,2,3	NTF	Unclass-Secret
Parsons	Steve Otsuki	NTBIC Sub SDT	F19628-88-C-0012	O	Facilities	Type 1	NTF	Unclassified
TASC	Capt. Shirley	SDIO/TND TND	SDIO-84-87-C-0001	T	Starlab/Directed Energy	Type 1,2,3	NTF	Unclass-Secret
Telos	Steve Otsuki	Hughes Sub SDT	F19628-88-C-0012	O	Ada Progamming Consultant	Type 1,2	NTF	Unclass-Secret
Vanguard Research	Nat Sojourner	NTBJPO SDT	SDIO-84-90-C-0028	O	NTBJPO SETA Support	Type 1,2	NTF	Unclass-Secret
FUTURE EXTERNAL								
Astronautics Lab (AFSC)	Capt. Tillon	SDIO/TNS TNS	F04611-86-C-0087	T	Radiation Signature Predictions	Type 1,2	SSD-T1	Unclass - Secret
BDM International	LtCol. Skvarenla	SDIO/ENA AQ	SDIO-84-88-C-0017	S	SODSIM Evaluation	Type 1,2	SDIO	Unclass - Secret
Directed Energy	Col. Myers	SDIO/TND TND	Gov't Agency	T	Directed Energy Experiment Support	Type 1,2,3	SDC, NTF, SDIO	Unclass - Secret
CSTC/Space Test Range	Col. Koval	NTBJPO SDT	Gov't Agency	T	Analysis of Space Safety & Hazards	Type 1,2	SSD	Secret
Integrated System Test	Dr. Carlson	SDIO/PT SDA	Gov't Agency	S	IST Framework Feasibility Demo	Type 1,2,3	NTF,SDC,SSD,SDIO,GE	Unclass - Secret
Lockheed	Dr. D. McClure	USASDC TNK	DASG-60-90-C-0011	T	Aerothermal Research	Type 1,2	SSD	Secret
Logistics Modelling	Allan Leary	SDIO/ENE SDA	Gov't Agency	S	SDS Logistics Modelling	Type 1,2	NTF,SDIO,SSD,SDC	Secret
McDonald Douglas	Col. Nagy	SDIO/ENS SDA	SDIO-84-88-C-0020	S	Threat and Architecture Analysis	Type 1,2	Dial-up	Secret
Special Programs Center	Dr. Carlson	SDIO/PT SDA	Gov't Agency	S	Special Programs Center (Threat)	Type 1,2	NTF,SDIO,SDC,SSD,SAC,GE	Secret
SPIET	Maj. Cox SDN	USASDC-SA-EV	DASG-60-87-0042	T	Survivability Planning Intercept Eval.	Type 1,2	SDC	Secret
SSD/CN	Dr. Carlson	SDIO/PT SDA	Gov't Agency	S	L1, L2 System Sim. Development	Type 1,2,3	SSD-T1	Secret
SSD/XRP	Allan Leary	SDIO/ENE SDA	Gov't Agency	B	Space-Based Element Development	Type 1,2	SSD	Secret
System Technology, Inc	Bob Cooley	USASDC SDN	DASG-60-89-C-0055	B	Fluid Dynamics for E2I and HEDI	Type 1,2	SDC	Secret
TASC	A. Griffiss TND?	RADC/OSCA	F30602-89-C-0064	T	DE Simulation Environment at RADC	Type 1,2	RADC (56kb-T1)	Secret
Army Space Command	Dr. Carlson	SDIO/PT SDA	Gov't Agency	S	C2 Gaming, Distributed Simulation	Type 1,3	PAFB - T1	Secret
W.J. Schafer Assoc.	Capt. Shirley	SDIO/TND TND	SDIO-84-88-C-0056	T	DE Experiment Support (Alpha Laser)	Type 1,2,3	NTF or ? - T1	Unclass - Secret
FUTURE INTERNAL								
NTBJPO - Current Operations	Col. Koval	NTBJPO SDT	Gov't Agency	O	JPO Operations/Admin	Type 1	NTF	Unclass
NTBJPO - Resource Mgmt	Col. Koval	NTBJPO SDT	Gov't Agency	O	Resource Mgmt/Resource Account.	Type 1	All Nodes	Unclass - Confid.
NTBJPO - Envr. Studies	Col. Koval	NTBJPO SDT	Gov't Agency	T	SDS Nuclear/Natural Environments	Type 1,2	NTF	Secret
NTBJPO - SSGM	Col. Koval	NTBJPO SDT	Gov't Agency	T	Strategic Scene Generation Model	Type 1,2	NTF	Secret
NTBJPO - Comm Tiger Team	Col. Koval	NTBJPO SDT	Gov't Agency	O	Tracking of NCG Database	Type 1	NTF	Unclass/Propr.
NTBJPO - User Services	Col. Koval	NTBJPO SDT	Gov't Agency	O	NTB User Services	Type 1	NTF	Unclass - Secret
NTBJPO - L1 Users Manual	Col. Koval	NTBJPO SDT	Gov't Agency	O	Level 1, Build 1 Users Manual	Type 1,2	NTF	Secret
UNVERIFIED FUTURE POINTS								

REV 2

User Organization	Sponsor	Sponsor Org	Contract #	Type	Function	User Type	Node/Data Rate	Exp. Security
Blue Forces			Gov't Agency	S				
Brilliant Pebbles Task Force			Gov't Agency	B				
OCE			Gov't Agency	B				
Innovative Science and Tech.			Gov't Agency	T				
KHILS (AFATL/SAI)	CDR. Korejwo	SDIO/TNS TNC	Gov't Agency	T				
Media Lab	Col. Koval	NTBJPO SDT	Gov't Agency	O				
MSX			Gov't Agency	T				
Security Network Architectur	Col. Koval	NTBJPO SDT	Gov't Agency	O				
Studies and Analysis	Col. Koval	NTBJPO SDT	Gov't Agency	S				
Technical Insertion Lab	Col. Koval	NTBJPO SDT	Gov't Agency	O				
US/UK			Gov't Agency	S				
KEY	Function Types		User Types					
	S - System		1 - Administrative, Data Exchange					
	B - Subsystem/Element		2 - Model Development/Batch Simulations					
	T - Technology		3 - Interactive, Distributive, or Real-Time Sims/Experiments					
	O - Other							

APPENDIX C

USASDC User Requirements

Requirements Data from USASDC PMAs

[illegible] CONCEPT / FUNCTIONS	PARTICIPANTS	LEVEL OF SECURITY	COMM REQ.	REMARKS	Use Th.
Computer Resources + Engr Office		SECRET	T3 / data	A03306	
High speed data transfer between CREO sites	SDC(CREO), Colsa, Inc			p. 2 SDN?	1
Unclassified Network Connect [illegible] sites	SDC(CREO) TBE, Colsa, Inc.	Unclass.	56 KB/s data	p. 3 SDN?	1
[illegible], Maintain, Operate Integration [illegible] SW/HW					
- Gen. Purp. Data Link for interactive data analysis/transfer between [illegible]-site users	(CSSD-SA-BB), SABMTBE, GBR	?	T1 data/voice	p11 A3306 SDN?	1, 2
[illegible] Engineering + Devmt.					
- [illegible] Link for developing [illegible] software and [illegible] system tests.	([illegible]) OTI, Colsa Inc.	Unclass.	T1 current 756Kb/s [illegible] data	A3306 p. 15 SDN?	1, 3
[illegible]/Technology Engr. Shd. [illegible] Base Element Devmt.	(CSSD-SA BB) MICOM	Unclass.	56 KB/sec data	p. 19 A2103, 2101, 2202 SDN	1, 2
[illegible] System Development [illegible] EADTB Node Interactive Test	(CSSD-SA BB) Hughes Aircraft, TRW, USA	Secret	T1 data	p. 24 A3305 TD	1, 3
- EADTB Node at Eglin AFB, FL	HAC, TRW, USA	Secret	T1 data	p. 25 A3305 TD	1, 3
ISS					
[illegible] Eng., Analysis IS Comm. [illegible] Level 1, 2, SAS, etc.	(CSSD-SA BB), SDC, TBE(SETAC) Coleman, Nichols, SPARTA	Secret	T1 (shared) (current); T3KB + T1 (anticipated) data/voice	p. 1 A3308 TD	1, 2, 3

CONCEPT / FUNCTIONS	PARTICIPANTS	SECURITY	REQ	REMARKS		
[illegible] Engr./Analysis GBR Dev. Comm Link for developing, [illegible] evaluation of GBR [illegible] software	(CSSD-SA-BB) Raytheon	Secret	B? <56KN/s (anticipated) data	A2103 p.20 ~~14~~ SDN		1,3
[illegible] Link for TRW/GSTS [illegible] + Analysis	TRW	Secret	(anticipated) <56KB/Sec data	p.22 210[illegible] SDN		1,[illegible]
[illegible] Analysis, Testing, Evaluation [illegible] GSTS Data	(CSSD-SA BB)			A2103 SDN		1,2,3
[illegible] Analysis/Maint. MDC-GSTS Data	Rockwell	Secret	T1 data	p. 23		
[illegible] Function	SPARTA, Colsa,	Unclass	56 KB/S data	A2103, p.27 SDN	—	✓
[illegible] Engr/Anal. GBR Dev. [illegible] Link for developing, [illegible] evaluating GBR system	(CSSD-SA-BB) XONTECH	Secret	<56KB/sec (anticipated) data	A210[illegible], p.21 SDN		1,3 ✓
[illegible] Development BMC3 [illegible] Test + Experiment Link with Army Space Command	(CSSD-SA-BB) Colsa, TRW	Secret	9.6 KB data/voice	A2300, p.13 SDA		1,3 ✓
[illegible] Function	(CSSD SA BB), GRC, Colsa, SDC	Unclass	19.2 KB/sec. data	A2310, p.17 SDA	—	✓
[illegible] Development [illegible] Evaluate, [illegible] SW	(CSSD SA BB) TRW	Unclass.	19.2 KB/S	~~A2300~~ A2103 p.31 SDN		1,3 ✓
[illegible] System Engineering/Anal [illegible] Monitoring and Test [illegible]	(CSSD SA BB) TRW	Secret	T1	A2300 p.30 SDA		1,3

[illegible] CONCEPT FUNCTIONS	PARTICIPANTS	SECURITY	REQ. •	• REMARKS		TYPE
[illegible] System Analysis and Engr. Lvl II Sim Devmt. and Anal. [illegible] Studies/Simulation System	(CSSD-SA-BB) TBE, SDC	SECRET, UNCLASS.	T1 (current) 96KB/sec. (anticip.) data	A4201, p.16	SDA	1,2,
[illegible] Analysis + Engr of STB Surveillance Test Bed Engr. and Maint.	(CSSD-SA-BB) GE, SDC	Unclass.	T1 (antic.) data	A4201 p. 18?	SDA	could be SD if it is di[illegible] to A3111 1,
Surveillance Testbed Engr. and Maint.	GE	Secret	<56kb/s (antic.) data/voice	p28	SDA	1,
[illegible] Devmt., Test, + Eval. - STB [illegible] Engineering + Maint.	(CSSD-SA-BB) NRC	Unclass.	9.6KB/s data/voice	p.29 A4701	SDA	1,2,3
[illegible] [illegible] and Devmt. of [illegible] from Lockheed plant	(CSSD-SA-BB) Lockheed, TBE	Secret	9.6KB/s data	p. 9 A4201	SDA	1,2
[illegible] Integration + Testing [illegible] Comm Link for Integ./Test/Anal of SDI SW	(CSSD-SA-BB) TBE	Secret	56kB/s (anticip.) data	p.10 A4201	SDA	1,2,3
[illegible]ineering/Operation, + Maint. of MDC Comm Link to TBE Developer, for MDC Eng/G	(CSSD-SA-BB) TBE	Secret	T1 data	p.12 A1105	TNS	1,2,3
[illegible] [illegible], Test, Eval + Maint. of [illegible] Models	(CSSD-SA-BB) MEVATEC, Colsa	(current) Dial up 300-2400 (anticip.) 56 KB data	Secret	A1202 p. 5	TNC	1,2,3

[illegible]CEPT/FUNCTIONS	PARTICIPANTS	LEVEL OF SECURITY	COMM. REQ.	REMARKS	
[illegible] Anal. of KEW SW Systems [illegible] AFB FL Comm Link for [illegible] Maint Study of KEW SW systems	(CSSD-SA BS) USAF, Colsa	Secret	>56kb/sec (antic.) data	A1202 p.6 TNC	1,2
[illegible] LG/G Link for [illegible], eval., maint, and [illegible] of KEW SW System	(CSSD-SA BS) USAF, Colsa	Secret	>56kb/sec (anticip.) data	A1202 p.7 TNC	1,2
[illegible] Analysis KEW/SDI SW system Analysis, test, Devmt. KEW SW.	(CSSD SA BS) SDC, Colsa	Secret	9.6 (current) >56kb/sec (antic) data	A1202 p.8 TNC	1,2,3
[illegible] Analysis KEW SW Comm Link for [illegible], Anal, [illegible], devmt KEW SW.	(CSSD-SA BS) USAF	Secret	19.2kb/sec (current) >56kb/sec (antic) data	p.14 A1202 TNC	1,2,3
[illegible] Analysis of KEW Systems [illegible], AFB, [illegible] Link for devmt, maint, test of key Systems	(CSSD SA BS) USA	Secret	T1 (antic) data	p.26 A1202 TNC	1,2,3
[illegible] for SW Testing, [illegible] Maint.	(CSSD SA BS) TBC	Secret	? 9.6 - T1 data	p.4 A1301? TND	1,2

APPENDIX D

SEIC Top Level User Requirements

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/H. TILLEY

S4401

User Type
1, 3

TEST CONCEPT: DemVal Test Plans

LTC Michael McNulty
SD10/PT = SD10/SD

FUNCTIONS: Intra–element, Inter–element and Integrated System Level Test

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Real time Inter–element voice, data & Imagery

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET/TOP SECRET, SAR, SCI

USER COMMUNITY: Services, element project offices element contractors, NTF

TIME PHASING: At least two years before anything more than existing NTBN capability is required

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/M. Foti

S 53308

TEST CONCEPT: Level 2 System Simulator

SDA

User Type
1, 3

FUNCTIONS: System Operational Effectiveness
Element Interactions
Message Profiles/Loading/Timing
Sensor Tasking
Engagement Planning

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Data, imagery, interactive interface

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET, WNINTEL
T/S if Survivability Enhancement options are modeled - GFY93 (TBR)
Proprietary (eg. Competing BP contractors)

USER COMMUNITY: SEIC, NTBIC, SDIO, Element Project Offices, Element Contractors and SETAs, AF-SSD, USASDC, AF-ESD

TIME PHASING: Development beginning summer 1991

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/J. Jewitt

5 53109

TEST CONCEPT: System Communications Security requirement definition

George Hoover
DIRNSA
Ft Meade

LtCol Richard Ritter SDIO/ENE
now TDI?

FUNCTIONS: Define System COMSEC requirements

User Type
1

TYPES OF INFORMATION
TRANSFER
AND GROSS SIZING: Documentation

TYPES OF SECURITY
CLASSIFICATION REQUIRED: SECRET and TOP SECRET COMSEC

USER COMMUNITY: SEIC, SDIO, NSA

TIME PHASING: SECRET COMSEC 4Q GFY91
TOP SECRET in GFY92

vyp

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE TIGER TEAM

COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/E. Mahon

S3202

TEST CONCEPT: Mission Analysis S

Ms. Kathleen Ruemmele - TNE
SDIO/PTI
now SDA

User Type
1, 2

FUNCTIONS: Threat analysis and definition
Survivability analysis

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Data (Threat)

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET, WNINTEL, SAR T/S & SECRET Condor Nest

USER COMMUNITY: SEIC & Threat WG
SAIC/Huntsville
SSD Processing Center/Survivability Analysis Lab

TIME PHASING: 9FY91

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/C. Beatty

5

TEST CONCEPT: Level 1 System Simulator CDR Jerry M. Jenkins SDA Sys Eng. + Integration SDIO/ENS (53308 L255)	User Type 1, 2, 3
FUNCTIONS: System Operational Effectiveness — Top Secret Rqmt? Engagement Planning Scenarios Ed Bassett Sensor Tasking Scenarios Message Profiles/Loading/Timing Req'ts	
TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Data, imagery, interactive interface	
TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET, WNINTEL	
USER COMMUNITY: SEIC, NTBIC, SDIO, SDC, SSD	
TIME PHASING: Immediate and continuing	

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/R. Marsden

A3111

TEST CONCEPT: Surveillance Test Bed (STB) T TDS

User Type 1, 2, 3

Dale Moore
CSSD-SA-E
Huntsville

LtC Chris Johnson
Dep. for Engr.
SDIO/EN ← TDS

FUNCTIONS: Surveillance and tracking
Detailed discrimination models
Check out of element algorithms
Trade studies among element contractors (eg. BE)

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Data
Interactive interface

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET, WNINTEL
Proprietary data

USER COMMUNITY: SEIC, AF-SSD (BE Project Office), SDC/ARC

TIME PHASING: Currently under development/ partially usable now

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/S. Kaltnecker

TEST CONCEPT:	Communications Network Testbed TNC	S1405? User Type 1, 2, 3
S1405: CDR Henry A. Korejwo Sensor ~~Interceptor~~ Technology SDIO/-VS		
FUNCTIONS:	Message profiles, message receipt probability Link connectivity, routing constraints Human in control network management performance Data flow latency and loading	
TYPES OF INFORMATION TRANSFER AND GROSS SIZING:	Real time voice & data Possibly imagery	
TYPES OF SECURITY CLASSIFICATION REQUIRED:	SECRET, WNINTEL	
USER COMMUNITY:	SEIC, NTBIC, SDIO, USSPACECOM	
TIME PHASING:	GFY92 FOR CONNECTIVITY INTO NTB NETWORK	

- 3?

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

April 5, 1991
J. Swift/B. JAMES

S Kathleen Zuernele TNE 53202?
SDIO/PT

TEST CONCEPT: War Gaming / Command + Control Exercising ~~$2300?~~

LTC Rich Hochberg
SDIO/ENA

User Type
1,2,3

FUNCTIONS: Command and Control Scenarios
Decision Timeliness/Human in the Loop

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Voice, data, imagery
Real-time and playback - Every other month for 3 to 4 days
~~a Possibly~~ video in future? Chris Capitano looking @ using VTC network

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET WNINTEL/NOFORN

USER COMMUNITY: Space Commands (Unified + Services), SAC, ESD, NTBIC, SDIO, JCS, SEIC, SDC/ARC, Others?

TIME PHASING: Immediate and continuing

NTB COMMUNICATIONS AND SECURITY ARCHITECTURE
TIGER TEAM
COMMUNICATIONS REQUIREMENTS SURVEY FOR THE SEIC

TNE

April 5, 1991
J. Swift/S. Skerl

T Validation

S1702?-

TEST CONCEPT: Testbed Integration – Uses a testbed to validate other testbed

53303, 3304

rt/TNE
1702 - LtCol Haynard P. Ladner
SDIO/TNP Test Operations

SDIO/ENT-01C - new. TNE
Capt. Robert A. Roncace
Threat, Test, + Evaluation

User Type
1, 2, 3

FUNCTIONS: Validate testbed assumptions

TYPES OF INFORMATION TRANSFER AND GROSS SIZING: Data

TYPES OF SECURITY CLASSIFICATION REQUIRED: SECRET, WNINTEL
Possibly T/S and SAR

USER COMMUNITY: Level 1 System Simulator, Level 2 System Simulator
CNTB, STB and Command and Control Simulations (War-games)

TIME PHASING: GFY92

APPENDIX E

Requirements Database Sample

REPORT OF USER REQUIREMENTS BY OFFICE

OFFICE:
USER ORGANIZATION: LOCUS, INC.
SDIO SPONSOR: NELSON HEAD
CONTRACT NUMBER: PMA-W2300
FUNCTION TYPE: O
SDS FUNCTION: NRL COMPUTER NETWORKING SUPPORT
USER TYPE: 0
CURRENT NODE: LAN
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

OFFICE:
USER ORGANIZATION: MITRE-ARLINGTON
SDIO SPONSOR:
CONTRACT NUMBER:
FUNCTION TYPE: O
SDS FUNCTION: MITRE SDIO LIASON LONG RANGE PLANNING
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE:
USER ORGANIZATION: BRILLIANT PEBBLES TASK FORCE
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: B
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE:
USER ORGANIZATION: US/UK
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: S
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:

OFFICE:
USER ORGANIZATION: BLUE FORCES
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: S
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

OFFICE:
USER ORGANIZATION: INNOVATIVE SCIENCE AND TECH.
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: T
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

OFFICE:
USER ORGANIZATION: MS
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: T
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE:
USER ORGANIZATION: COE
SDIO SPONSOR:
CONTRACT NUMBER: GOV'T AGENCY
FUNCTION TYPE: B
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AC

FUNCTION TYPE: O
SDS FUNCTION: TEST AND EVALUATION ACTIVITY SUMMARY
USER TYPE: 1
CURRENT NODE: SDIO
CURRENT DATA RATE: T1
LOWEST SECURITY LEVEL: SECRET
HIGHEST SECURITY LEVEL: SECRET

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: SAIC
SDIO SPONSOR: LCOL.SKVARANINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE: B
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: NICHOLS RESEARCH
SDIO SPONSOR: LCOL.SKVARNINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE:
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: ANALYTIC SERVICES
SDIO SPONSOR: ON USER SUUPORT
CONTRACT NUMBER: NA
FUNCTION TYPE: S
SDS FUNCTION: SYSTEM ANALYSIS (SODSIM)
USER TYPE: 2
CURRENT NODE: SDIO
CURRENT DATA RATE:
LOWEST SECURITY LEVEL: NA
HIGHEST SECURITY LEVEL: NA

REPORT OF USER REQUIREMENTS BY OFFICE

E: AQ
USER ORGANIZATION: BLIME.INC.
SDIO SPONSOR: LTCOL SKVARNANINA
CONTRACT NUMBER: SDIO-84-88-C-0035
FUNCTION TYPE: S
SDS FUNCTION: SODSIM DEVELOPMENT SYS. ANALYSIS - SODSIM
USER TYPE

HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: BDW INTERN'L (SUPER SETA)
SDIO SPONSOR: LTCOL SKVARNANINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE: O
SDS FUNCTION: GPALS STUDIES/USER SURVEYS
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: COLEMAN RESEARCH CORP.
SDIO SPONSOR: LTCOL SKVARNANINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE:
SDS FUNCTION:
USER TYPE: 2
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FFICE: AQ
USER ORGANIZATION: W.J. SHAFER ASSOC.
SDIO SPONSOR: LCOL. SKAVARNINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE:
SDS FUNCTION:
USER TYPE:
CURRENT NODE:
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FICE: AQ
USER ORGANIZATION: BDM INTERNATIONAL
SDIO SPONSOR: LTCOL. SKVARENINA
CONTRACT NUMBER: SDIO-84-88-C-0017
FUNCTION TYPE: S
SDS FUNCTION: SODSIM EVALUATION
USER TYPE: 2
CURRENT NODE: SDIO
CURRENT DATA RATE:
LOWEST SECURITY LEVEL: UNCLASS
HIGHEST SECURITY LEVEL: SECRET

REPORT OF USER REQUIREMENTS BY OFFICE

USER ORGANIZATION: BOOZ, ALLEN, & HAMILTON
SDIO SPONSOR: BILLY LOVE
CONTRACT NUMBER: SDIO-84-88-C-0019
FUNCTION TYPE: O
SDS FUNCTION: PLANNING AND CONTROL
USER TYPE: 1
CURRENT NODE: SDIO
CURRENT DATA RATE:
LOWEST SECURITY LEVEL:
HIGHEST SECURITY LEVEL:

REPORT OF USER REQUIREMENTS BY OFFICE

FICE: POE
USER ORGANIZATION: APPLIED RESEARCH-ARLINGTON
SDIO SPONSOR: JAMES DRYDEN
CONTRACT NUMBER: SDIO-84-88-C-0018
FUNCTION TYPE: S
SDS FUNCTION: ARCHITECTURE ANALYSIS
USER TYPE: 2
CURRENT NODE: SDIO
CURRENT DATA RATE:
LOWEST SECURITY LEVEL: SECRET
HIGHEST SECURITY LEVEL: SECRET

REPORT OF USER REQUIREMENTS BY OFFICE

FICE: POE
USER ORGANIZATION: DECISION SCIENCE APPLIC.
DIO SPONSOR: JAMES DRYDEN
CONTRACT NUMBER: SDIO-84-88-C-0018
FUNCTION TYPE: S
SDS FUNCTION: EFFECTIVENESS MODELS (SODSIM)
USER TYPE: 2
CURRENT NODE: SDIO
CURRENT DATA RATE: DIAL UP
LOWEST SECURITY LEVEL: SECRET
HIGHEST SECURITY LEVEL: SECRET

REPORT OF USER REQUIREMENTS BY OFFICE

FICE: POE
USER ORGANIZATION: SRS TECHNOLOGIES-ARLINGTON
SDIO SPONSOR:
CONTRACT NUMBER: SDIO-84-88-C-0019
FUNCTION TYPE: S
SDS FUNCTION: MEM SODSIM ANALYSIS
USER TYPE: 2
CURRENT NODE: SDIO
CURRENT DATA RATE: TI
LOWEST SECURITY LEVEL: SECRET/NOF/CNWDI/WNINTEL
HIGHEST SECURITY LEVEL: SECRET/NOF/CNWDI/WNINTEL

REPORT OF USER REQUIREMENTS BY OFFICE

ICE: POE
USER ORGANIZATION: TASC-ARLINGTON(SUPERSETA)
SDIO SPONSOR: JAMES DRYDEN
CONTRACT NUMBER: SDIO-84-88-[illegible]

APPENDIX F

High-Level User View

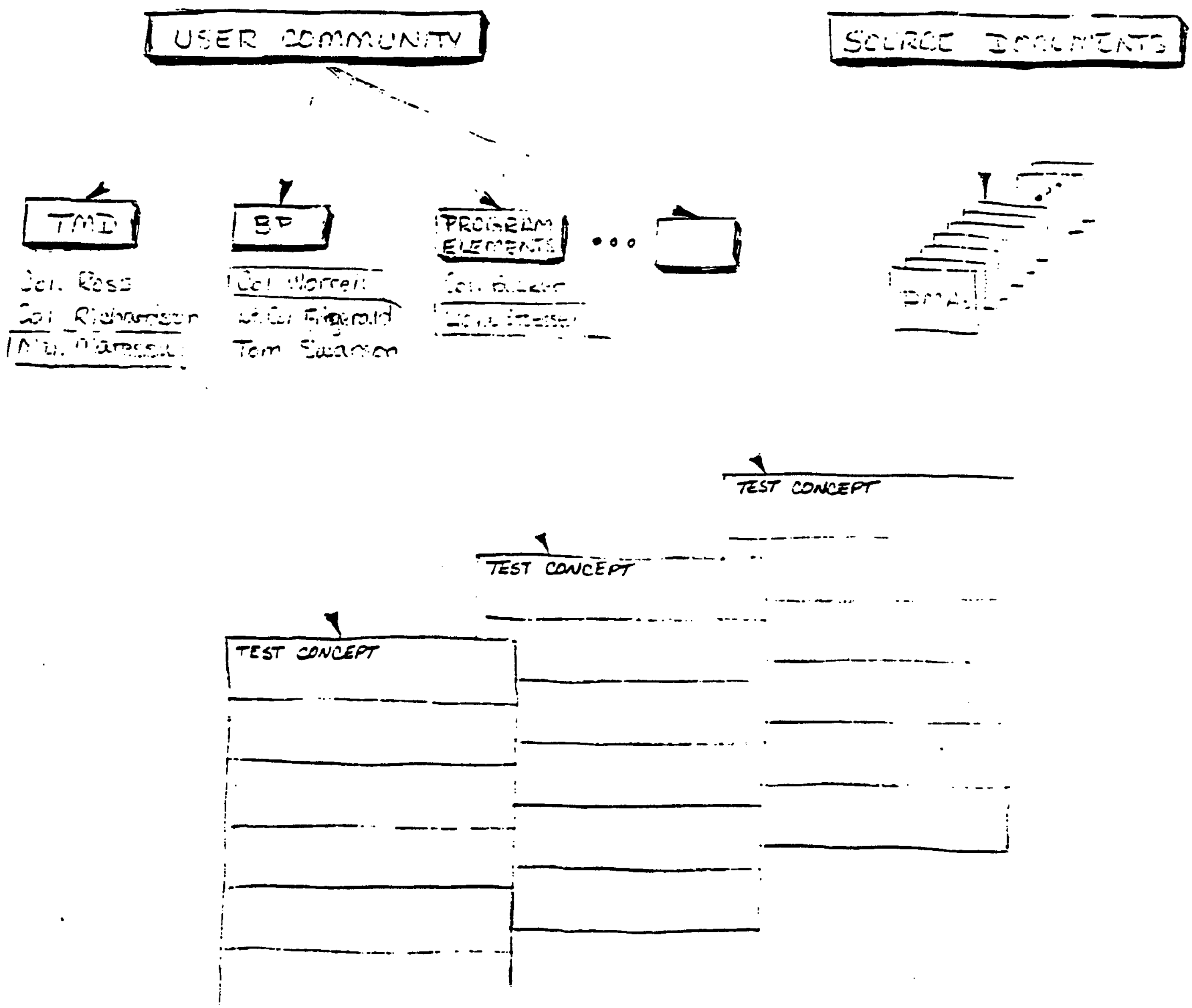
SDIO

THE HIGH-LEVEL USER VIEW

4/2/91

REQUIREMENTS COMPILATION

SOURCE OF INFORMATION



4/3/91

TEST CONCEPT

FOR:
- TMD-GBR
- ACTS
- P^3I, PAC II
- ARROW
- ERINT
- ACES
- THAAD

(1) CONCEPT DEFINITION/DEVELOPMENT TESTING - STANDALONE

(2) OPERATIONAL TESTING - SYSTEM ELEMENT - STANDALONE

(3) OPERATIONAL TESTING - INTEGRATED SYSTEM - FULLY CONNECTED AS REQUIRED

FUNCTIONS

SENSORS

SPACE SENSORS   TMD-GBR

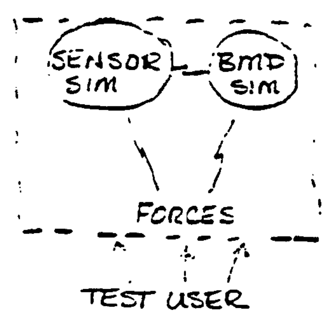
TACTICAL/THEATER BALLISTIC MISSILE DEFENSE COMPONENTS:

ACES   THAAD
ERINT
ARROW
P^3I, PAC II
ACTS

MILITARY FORCES - COMMAND AND CONTROL:

GROUND TROOPS
AIRCRAFT
SHIPS

TYPES OF INFORMATION TRANSFER



(1) SIMULATION TO SIMULATION (HIGH SPEED) WITHIN THE SAME FACILITY or simulation to prototype

(2) SIMULATION TO PROTOTYPE
PROTOTYPE TO PROTOTYPE } UNDEFINED

(3) INTERFACE TO STRATEGIC } UNDEFINED

TYPES OF SECURITY

UNDEFINED, HOWEVER CAN PROJECT - SECRET AT A MINIMUM
- ALLIED PARTICIPATION MUST BE SEGMENTE

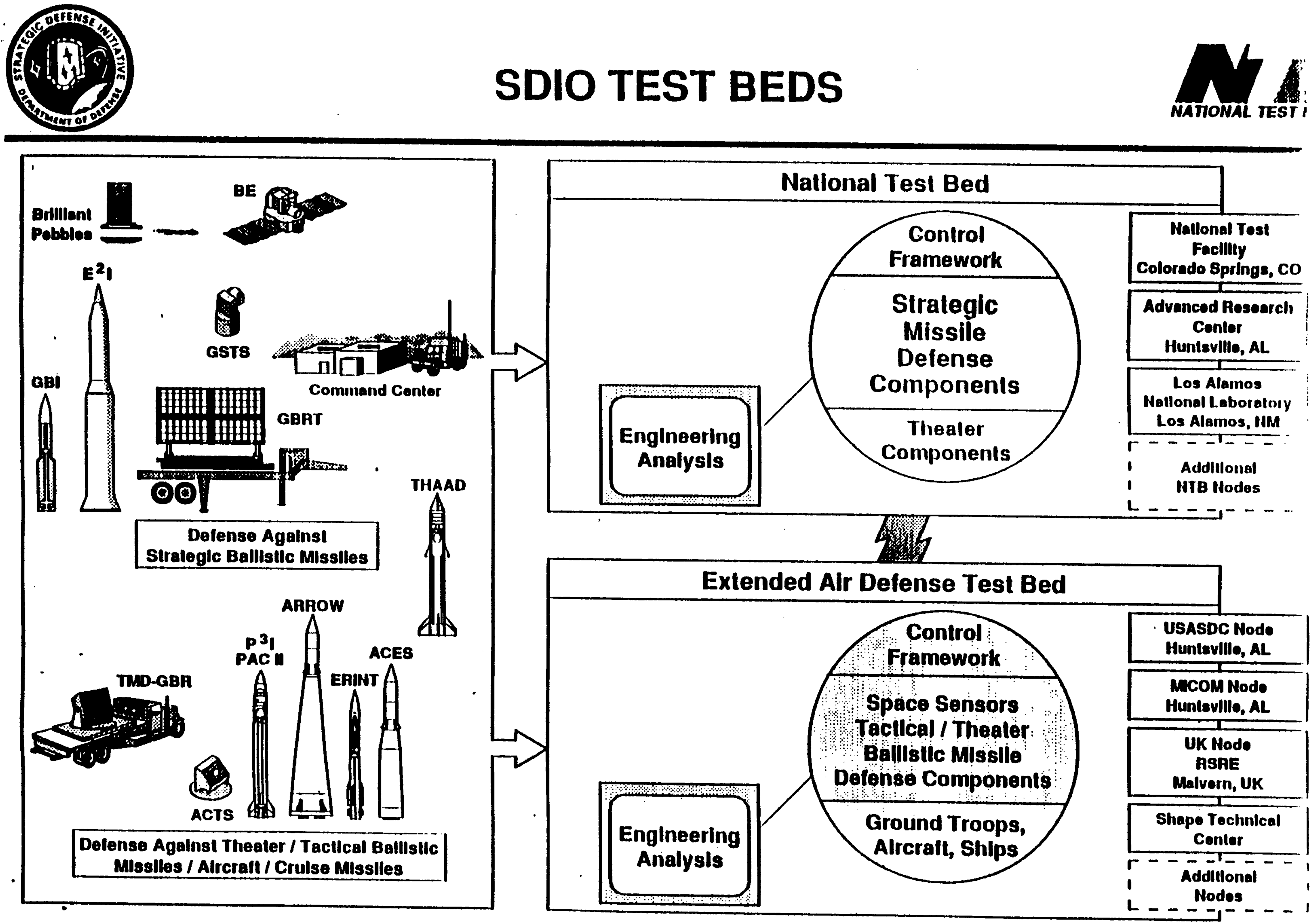
USER COMMUNITY

USASDC, MICOM, SHAPE, UK, OTHER US ARMY, WHITE SANDS (TECHNICALLY NOT A USER)

TIME PHASING

"2 YEARS FROM NOW" FOR (1)

SDIO TEST BEDS



jm-14757A / 0

TEST CONCEPT

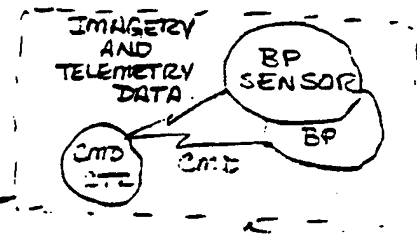
BRILLIANT PEBBLES TESTS
- (1) DESIGN/ANALYSIS TRADE-OFFS AND TESTS, OPERATOR TESTS
- (2) DT & E
- (3) OT & E
- (4) FOLLOW-ON T+E/LC TESTING

FUNCTIONS

BP SENSOR
COMMAND CENTER
COMMAND CENTER LINKS FOR C^2 AND MONITORING DATA

TYPES OF INFORMATION TRANSFER

(1) SIMULATION TO SIMULATION
(2), (3), (4) PROTOTYPE TO SIMULATION
PROTOTYPE TO PROTOTYPE



(1)-(4) PRE FSD, FSD CONTRACTORS
BPTF, SE @ PENTAGON
(3) ADD AFOTEC

- IMAGERY AND TELEMETRY DATA TO COMMAND CTR
- REAL TIME DATA ON KILL EFFECTIVENESS AND SHOT OPPORTUNITIES
- PERIODIC UPDATE ON THREAT DATA FROM GROUND CONTROLLERS
- PERIODIC UPLOAD OF SOFTWARE FROM COMMAND CENTER TO BP

TYPES OF SECURITY

SECRET IN GENERAL
GO COMMAND- "ENCRYPTED"
CONTROL SOFTWARE- "ENCRYPTED"

USER COMMUNITY

BPTF (PENTAGON & COLORADO SPRINGS) AND SETA'S (CURRENTLY BDM AND TASC)
SE
OTHER ELEMENTS
OPERATORS (FOR TRAINING)
PRE-FSD/FSD CONTRACTORS
CAIG
LLL
COMMAND CENTER
POSSIBLY TACTICAL COMMANDERS, THEATER CINCS/ALLIES

TIME PHASING

(1) 1991-93
(2) 94-95
(3) 96-97

BP
3/28/91

OTHER COMMENTS

- NEED NTB TO TEST INTERCONSTELLATION COMMUNICATIONS CONCEPT
- TEST TARGET TRACKING AND ROBUSTNESS OF THE CAPABILITY
- COULD USE NTB TO SIMULATE WORKLOAD ON GROUND CREWS AND DETERMINE HOW MUCH CONTROLLERS CAN HANDLE
- NEED NTB TO RUN ORDER OF FLIGHT TESTS (MAYBE A NEW FACILITY
- REALLY NEED NTB FOR SENSITIVITY STUDIES ON SYSTEM EFFECTIVENESS (ESPECIALLY IF THERE IS A FLY-OFF)

LONG TERM

- NEED FULL SIMULATION CAPABILITY
- NEED TO BE ABLE TO DO ELEMENT WITHIN ELEMENT TRADES
- DETERMINE BLOCK UPGRADES – EVALUATE BEFORE IMPLEMENT
- SUPPORT TRAINING

⟹ NTB SHOULD SUPPORT CHANGING MODULES

- THREAT
- ENVIRONMENT
- COMPONENT

Test Concept

All Elements less BP & TMD
Element simulation

Functions

Sensor data to element components
BSTS
GBR } E^2I / GBI
SSTS

Command and Control

Types of Information Transfer

- Simulation to Simulation (High speed)
  special purpose equipment - All in same facility -
  All by single Contractor

  Had attempted to use NTB to move data between facilities but was denied by the System Engineer.

  No Need for NTF Computers or capability

  Future requirements - No comment - suggested we discuss with the specific elements and their contractors

Types of Security
Suggested we discuss with specific elements

User community
USASDC, Space command, [redacted]

Time Phasing: Simulation to Simulation - Now

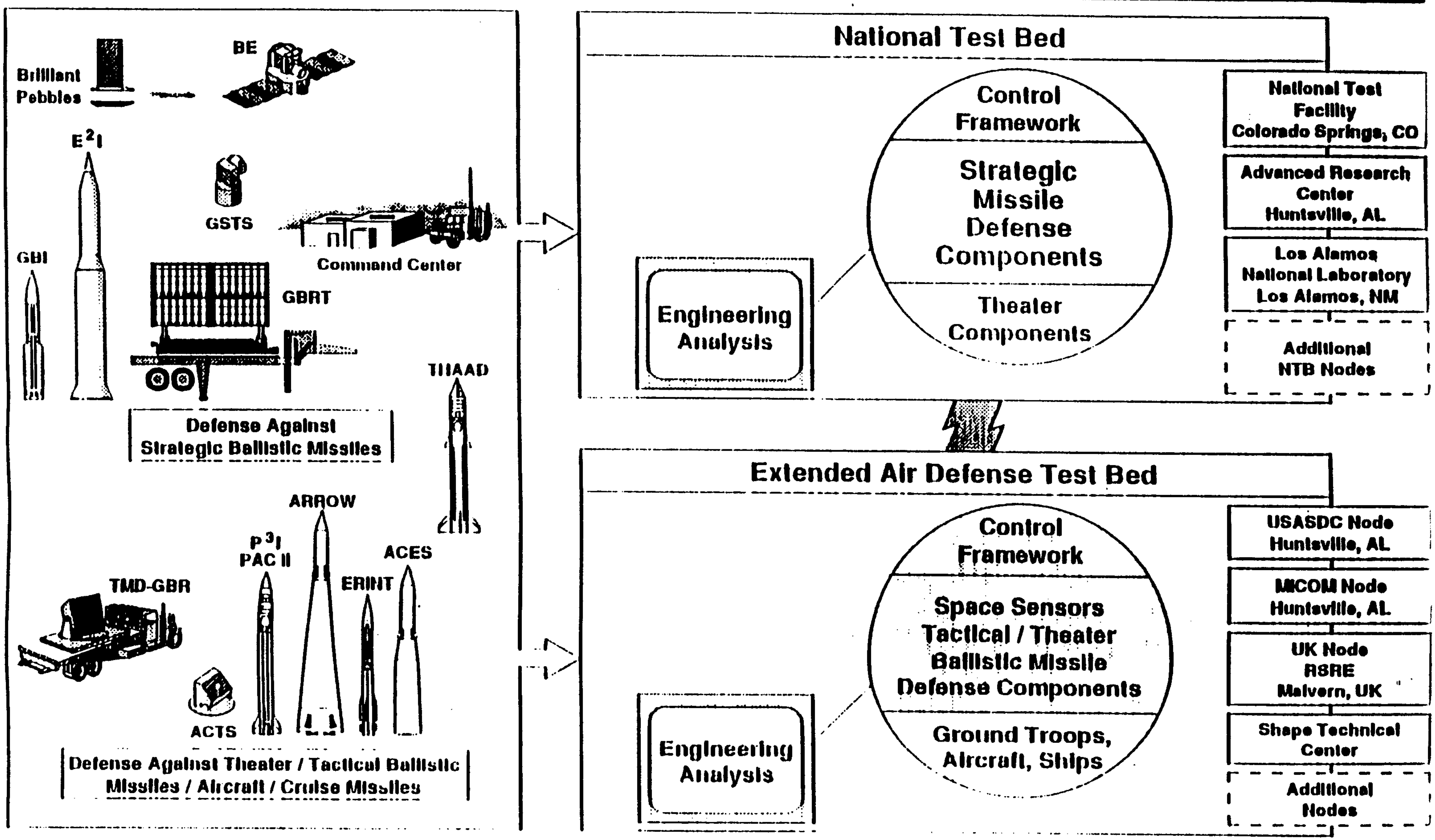
RESULTS OF PMA DATABASE SURVEY

- o Unclassified database extract of ~~195~~ 186 PMAs was printed out April 3 and analyzed April 4-5
- o Each PMA extract included PMA number, title, Executing Agent, security classification, technical objectives and (if unclassified) technical description
- o Analysis was useful for the following reasons:
  - It summarized all SDIO programs, showing where different organizations in different locations are performing related work.
  - For some projects, PMAs specifically referenced requirements to interact with other programs and requirements to perform tests.
  - Results can be used to check completeness of data collection efforts performed by other Working Group members
- o PMAs do not contain information at the level of detail required to fill out Working Group's survey form.

RESULTS OF TMD INTERVIEW (MAJ. F. MARESSA)

- o Program currently in requirements definition phase for simulation software
- o Plans to use ARC for simulation hardware platform (Extended Air Defense Test Bed)
- o Test plans were prepared 2 to 3 years ago and included in annex to Anser/MITRE document. Test concepts have not been reformulated to reflect recent program redirectior
- o Doesn't see NTB involvement in details of air defense simulations; some overlap anticipated at Theater level; envisions interprocessor link to achieve interface
- o Sees role of NTB to provide high-fidelity representation of strategic systems for use in TMD simulations

SDIO TEST BEDS



jm 14757

ANNEX 2

Technology Survey

ANNEX 2

TECHNOLOGIES

May 10, 1991

I. INTRODUCTION

The purpose of this annex is to assemble and organize information which will assist the NTBN Security and Communications Architecture Working Group (Tiger Team) in developing architectures which meet NTBN system requirements. This annex was prepared by a Technology Group working as an integral part of the Tiger Team, whose overall goal is to prepare near-term and long-term recommendations for upgrading NTBN security and communications capabilities. In support of this goal, the Technology Group's objectives were defined as follows:

1) To document the baseline NTBN configuration;

2) To review technology documentation previously distributed to Tiger Team members;

3) To collect additional information on products and technologies with potential application to NTBN upgrades;

4) To prepare summary tables and graphics which would assist Tiger Team members in relating the technology information to NTBN requirements; and

5) To write a final report for review by Tiger Team members in preparation for subsequent Tiger Team meetings.

The group's work focused on LAN and WAN technologies, not products such as trusted operating systems, compartmented mode workstations, DBMSs or access control subsystems which enhance the security of the individual hosts interconnected by LANs and WANs.

II. METHODOLOGY

Technology Group members held an organizational meeting on April 9, 1991. At this meeting and in subsequent VTC/telephone discussions, members agreed on an approach to accomplishing the group's five objectives. This approach included the following tasks:

1) Baseline Architecture. Previously prepared NTBN documentation was analyzed to prepare a simple set of diagrams showing the existing NTBN design. Responsibility for this task was assigned to J. Brewer and P. Burian.

2) Documentation Review. Technology surveys distributed at the March 11-12, 1991 Working Group meeting were reviewed for information applicable to the NTBN architecture development effort. Responsibility for this task was assigned to T. Bailey. The following specific documents were reviewed:

a) Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program (October 10, 1990);

b) Secure LAN Product Analysis for the NTBN (January 9, 1991);

c) NTB Security Strategy Working Group Draft Report (March 4, 1991); and

d) Security Technology Evaluation Report (NTB Technical Report for TRN 0012-NTB-90-027 dated October 31, 1990).

3) Product and Technology Data Collection. All members collected product and technology data not previously presented to the working group. Data sources included:

a) Technology symposia sponsored recently by NTBJPO and NTBIC;

b) The January 1991 edition of NSA's Information Systems Security Products and Services Catalogue, and the April 1991 Supplement to the same document.

c) WAN Components Specification, prepared by NSA Network Project Management Office;

d) Technical information obtained directly from vendors; and

e) Data which Technology Group members have access to through their participation in other secure networking projects.

4) Data Analysis and Reduction. The information collected in steps 1, 2, and 3 above was analyzed and presented in tabular and graphical formats to facilitate discussions of alternative architectures. Tables divided products into categories, summarized their characteristics, and compared their ability to meet perceived NTBN communications and security requirements. Graphics showed how available products fit into generic network architectures. Responsibility for this task was shared by J. Brewer, P. Burian and T. Bailey.

5) Final Report. Results of the Technology Group's efforts were collected in this report. The detailed results are provided as a set of appendices. A brief summary is given in the following paragraph.

III. SUMMARY OF RESULTS

The following appendices to this report are provided to the Security and Communications Architecture Working Group as tools to facilitate development of near-term and long-term NTBN architectures:

1) Appendix A--Baseline Architecture Diagrams. Two figures are provided. Figure A-1 summarizes the AIS components and tail circuits at NTBN nodes. Figure A-2 shows the existing wide area network communications architecture which interconnects the nodes.

2) Appendix B--Evaluated Products List. Material was extracted from the January 1991 Evaluated Products List and annotated to include EPL changes through March 1, 1991 as documented in the April 1991 EPL supplement. The EPL defines four classes of products: 1) Unix-like Systems (including Compartmented Mode Workstations); 2) Proprietary (i.e., non-Unix) Systems; 3) Networks and Network Components; and 4) Subsystems. Trusted database management systems are not currently included on the EPL.

3) Appendix C--Secure Networking Product Summary. Information on networking products surveyed in Task 2 and Task 3 above is summarized in tabular format. Table C-1 divides networking products into four categories based on whether or not Type 1 encryption and/or trusted software are designed into the product. Table C-2 describes how each of these products is used in a secure LAN or WAN environment. Table C-3 compares product features and specifications which are relevant to the NTBN architecture development task.

4) Appendix D--WAN Product Data. SDIO's NSA representatives furnished this data on products currently in use in DoD WANs.

5) Appendix E--Technology Briefing. This is a presentation prepared by the NTB integration contractor. It summarizes information presented at various technology symposiums sponsored by the NTBJPO.

6) Appendix F--Generic Architecture Diagrams--Graphics showing how products described in Appendix C are used in LAN and WAN architectures. These diagrams are taken from vendor literature, Government briefings, and documents analyzing available network security products.

APPENDIX A

BASELINE ARCHITECTURE DIAGRAMS

NTBN ARCHITECTURE

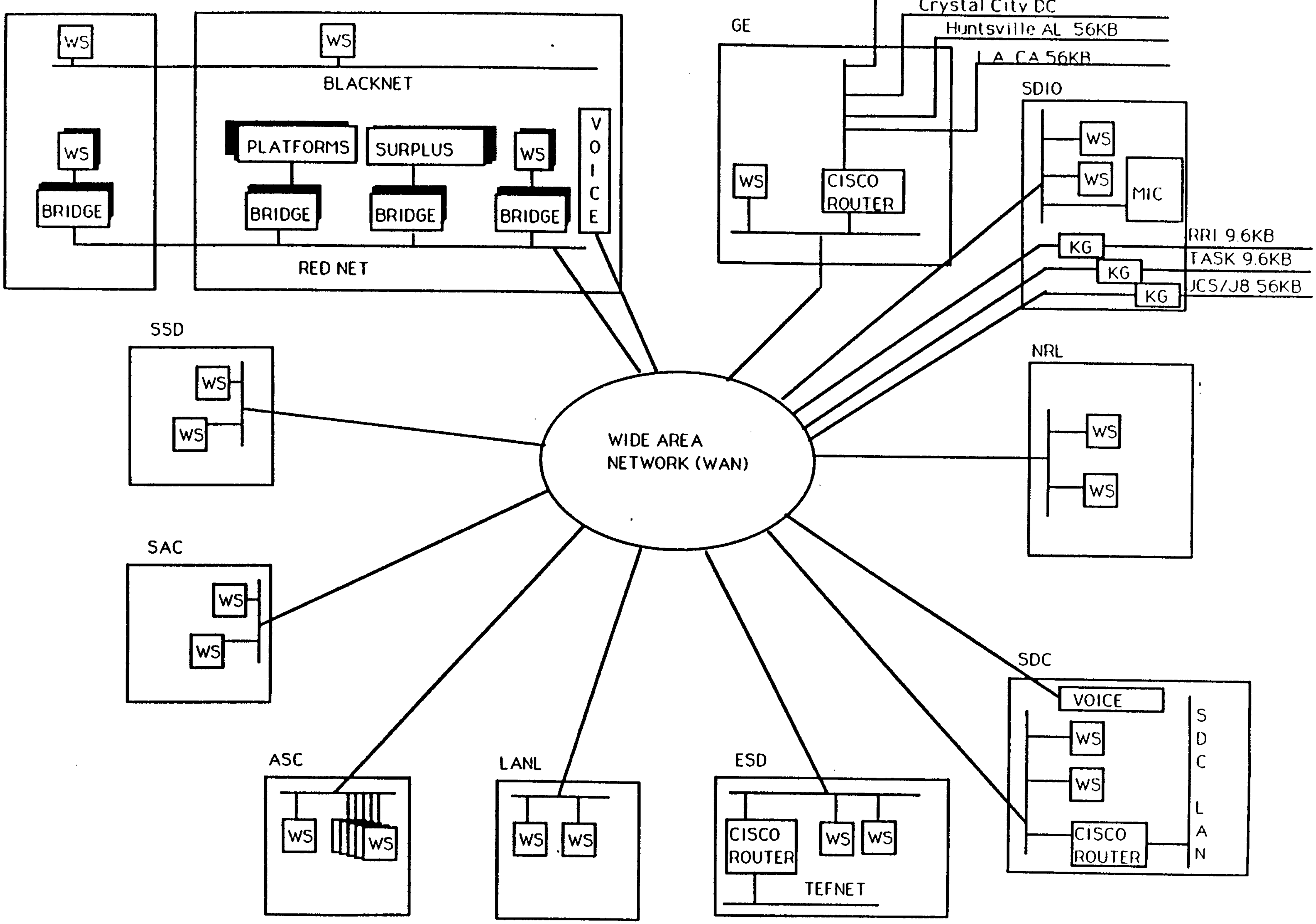


Figure A-1. NTBN Node Configuration

NTBN WAN

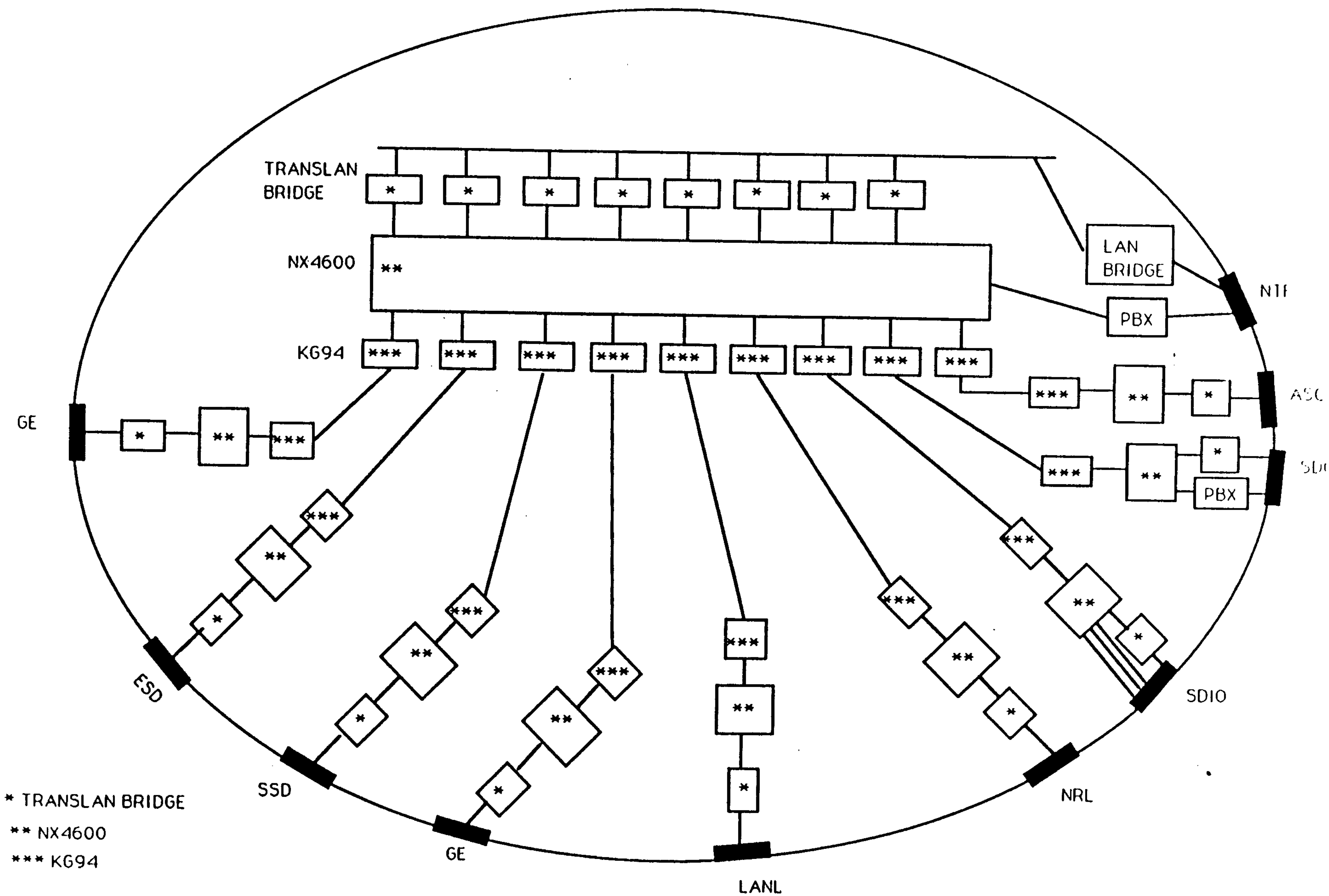


Figure A-2. Existing WAN Architecture

APPENDIX B

EVALUATED PRODUCTS LIST

Appendix B

JANUARY 1991

EVALUATED PRODUCTS LIST

for

TRUSTED COMPUTER SYSTEMS

Status As of 1 December 1990

With annotations showing
changes through March 1, 1991
as presented in April 1991
EPL Supplement

Reference to page in complete document

INDEX OF EVALUATIONS BY PHASE

I. Products in the Vendor Assistance Phase:

Vendor	Page
Amdahl Corporation	4-30
Convex Computer Corp	4-30
Harris Corporation	4-30
Silicon Graphics Inc.	4-30
Sun Microsystems	4-30
Cray Research Inc.	4-30
Loral Command and Control	4-30

II. Products in the Design Analysis Phase:

Vendor	Product	Candidate Division	Page
Addamax Corporation	System V UNIX System	B	4-32
	4.3BSD UNIX System	B	4-32
	Compartmented Mode Workstation	B	4-32
American Telephone and Telegraph Co.	UNIX V	B	4-32
Concurrent Computer Corporation	OS-32	C	4-32
Digital Equipment Corporation	Compartmented Mode Workstation	B	4-32
	SE-VMS	C/B	4-32
Gemini Computers, Inc.	GEMSOS	A	4-32
	M-COMPONENT	A	4-32
International Business Machines Corp	VM/SP	C/B	4-32
Sun Microsystems Federal, Inc.	Compartmented Mode Workstation	B	4-32
Tandem Computers, Inc.	Guardian-90	C	4-32

III. Products in Formal Evaluation:

Vendor	Product	Candidate Level of Trust	Page
Boeing Aerospace	SNS SNS + NM	A1	4-44
HFSI, Inc	XTS-200	B3	4-52
~~Secureware, Inc.~~	~~Compartmented Mode Workstation~~	~~B1~~ Completed 1/30/91	~~4-49~~
~~Trusted Information Systems, Inc~~	~~Trusted XENIX~~	~~B2~~ Completed 1/22/91	~~4-46~~

IV. Evaluated Systems and Add-On Packages:

Vendor	Product	Level of Trust	Page
American Telephone & Telegraph (AT&T)	System V/MLS	B1	4-82
Computer Associates International	ACF2/MVS	C2	4-104
	ACF2/VM	C2	4-69
	Top Secret	C2	4-106
Control Data Corp.	NOS	C2	4-60
Data General Corp.	AOS/VS	C2	4-79
Digital Equipment Corp.	VAX/VMS 4.3	C2	4-62
Gould, Inc., Computer Systems Division	UTX/32S	C2	4-65
Hewlett Packard Computer Systems Div.	MPE V/E	C2	4-77
Honeywell Information Systems, Inc.	Multics	B2	4-58
	SCOMP	A1	4-56

Vendor	Product	Level of Trust	Page
International Business Machines Corp.			
	MVS/RACF	C1	4-102
	MVS/XA/RACF	C2	4-72
	VM/SP with RACF	C2	4-88
	MVS/ESA	B1	4-95
Trusted Information Systems	Trusted Xenix V2.0	B2	April 91, 4-5-20
Prime Computer, Inc.	Primos	C2	4-75
Secureware, Inc.	CMW	B1	April 91, 4-5 20
Unisys Corp.	A Series	C2	4-67
	OS 1100	B1	4-85
Verdix Corp.	VSLAN 5.0	B2 MAID	4-91
Wang Laboratories	SVS/OS CAP 1.0	C2	4-99

V. Evaluated Subsystems:

ALC Stealth Group	Tigersafe	I&A / D; OR / D	4-128
	Tigersafe 3.03.1EN	I&A / D; OR / D	4-137
Clyde Digital Systems	Dialback	Subsystem	4-123
Codercard, Inc.	CPP-300	Subsystem	4-111
Computer Accessories, Inc	Private Access	Subsystem	4-122
Computer Security Corp.	Citadel	Subsystem	4-124
	Sentinel	Subsystem	4-116
Cortana Systems Corp.	PC Security	Subsystem	4-120
Enigma Logic, Inc.	Safeword	Subsystem	4-115
E-X-E Software Inc.	OnGuard	I&A/D1:DAC/D1	4-136
Eyedentify Inc.	EIS	I&A / D1	4-139
Fischer International	Watchdog	Subsystem	4-112
	Watchdog Armor	I&A/D1; DAC/D2; AUD / D2; OR / D	1-141
Gordian Systems, Inc.	Access Key	Subsystem	4-110
IDENTIX Corp.	IDX-50	Subsystem	4-119
Infosafe Corp.	X-LOCK 50	Subsystem	4-125
Infotron	INX 4400	I&A / D	4-126
Key Concepts, Inc.	SureKey	Subsystem	4-118
Micronyx, Inc.	Triad Plus	Subsystem	4-117
	TriSpan	I&A / D; DAC / D; AUD / D	4-130
Pyramid Development Corp.			
	PC/DACS	I&A/D; DAC/D; AUD/D; OR/D	4-134
Security Dynamics, Inc.	ACE	Subsystem	4-114
Spectrum Manufacturing, Inc.			
	DPS 800/12	Subsystem	4-121
Sytek, Inc.	PFX Passport	Subsystem	4-113
Wang Laboratories	MicroControl	I&A / D; DAC / D; AUD / D	4-132

INDEX OF Completed AND Formal EVALUATIONS BY LEVEL OF TRUST

C2: (cont.)

Vendor	Product	Evaluation Status	Page
Control Data Corporation	NOS	Completed	4-60
Data General Corp.	AOS/VS	Completed	4-79
Digital Equipment Corporation	VAX/VMS 4.3	Completed	4-62
Gould, Inc., Computer Systems Division	UTX/32S	Completed	4-65
Hewlett Packard Computer Systems Div.	MPE V/E	Completed	4-77
International Business Machines Corp.	MVS/XA with RACF	Completed	4-72
	VM/SP with RACF	Completed	4-88
Prime Computer, Inc.	Primos	Completed	4-75
Unisys Corp.	A Series	Completed	4-65
Wang Laboratories, Inc.	SVS/OS	Completed	4-99

B1:

Vendor	Product	Evaluation Status	Page
American Telephone and Telegraph Co.	System V/MLS	Completed	4-82
International Business Machines Corp.	MVS-ESA	Completed	4-95
Secureware, Inc.	Compartmented Mode Workstation	~~Formal~~ Completed	4-49
Unisys Corp.	OS 1100	Completed	4-85

B2:

Vendor	Product	Evaluation Status	Page
Honeywell Information Systems, Inc.	Multics	Completed	4-58
Trusted Information Systems, Inc.	Trusted XENIX	~~Formal~~ Completed	4-46
Verdix Corp.	VSLAN	Completed	4-91

B3:

Vendor	Product	Evaluation Status	Page
Honeywell Information Systems, Inc	XTS-200	Formal	4-52

A1:

Vendor	Product	Evaluation Status	Page
Boeing Aerospace	SNS SNS + NM	Formal	4-44
Honeywell Information Systems, Inc.	SCOMP	Completed	4-56

INDEX OF EVALUATED PRODUCTS AND PRODUCTS IN EVALUATION BY VENDOR

Vendor	Product/Product Type	Evaluation Status	Page
Cortana Systems Corp.	PC Security	Completed	4-120
Data General Corp	AOS/VS	Completed	4-79
Digital Equipment Corporation			
	VAX/VMS 4.3	Completed	4-62
	Compartmented Mode Workstation	DA	4-32
	SE-VMS	DA	4-32
Enigma Logic., Inc	Safeword	Completed	4-115
E-X-E Software Security	OnGuard	Completed	4-136
Eyedentify International Systems Corp			
	Eyedentify Information Security System (EIS)	Completed	4-139
Fischer International	Watchdog	Completed	4-112
	Watchdog Amor	Completed	4-141
Gemini Computers, Inc.	GEMSOS	DA	4-32
	M-Component	DA	4-32
Gordian Systems, Inc.	Access Key	Completed	4-110
Gould, Inc., Computer Systems Division			
	UTX/32S	Completed	4-65
Harris Corporation	Unix operating system	VAP	4-30
Hewlett Packard Computer Systems Div.			
	MPE V/E	Completed	4-77
Honeywell Information Systems, Inc.			
	Multics	Completed	4-58
	SCOMP	Completed	4-56
HFSI Inc.	XTS-200	Formal	4-52

Vendor	Product/Product Type	Evaluation Status	Page
International Business Machines Corp			
	MVS/RACF	Completed	4-102
	MVS/XA with RACF	Completed	4-72
	VM/SP with RACF	Completed	4-88
	MVS-ESA	Completed	4-95
	VM/SP	DA	4-32
IDENTIX Corp.	IDX-50	Completed	4-119
Infosafe Corp.	X-LOCK-50	Completed	4-125
Infotron	INX 4400	Completed	4-126
Key Concepts, Inc.	SureKey	Completed	4-118
Micronyx, Inc.	Triad Plus	Completed	4-117
	TriSpan	Completed	4-130
Prime Computer, Inc.	Primos	Completed	4-75
Pyramid Development Corp.			
	PC/DACS	Completed	4-134
Secureware, Inc.	Compartmented Mode Workstation	~~Formal~~ Completed	4-49
Security Dynamics, Inc.	ACE	Completed	4-114
Silicon Graphics Inc.	Unix operating system	VAP	4-30
Spectrum Manufacturing, Inc.			
	DPS 800/12	Completed	4-121
Sun Microsystems Federal, Inc.			
	Compartmented Mode Workstation	DA	4-32
	UNIX based Operating System	VAP	4-30
Sytek, Inc.	PFX Passport	Completed	4-113
Tandem Computers Inc.	Guardian-90	DA	4-32

Vendor	Product/Product Type	Evaluation Status	Page
Trusted Information Systems, Inc.			
	Trusted XENIX	Completed ~~Formal~~	4-46
Unisys Corp.	A Series	Completed	4-67
	OS 1100	Completed	4-85
Verdix Corp.	VSLAN	Completed	4-91
Wang Laboratories, Inc.	SVS/OS	Completed	4-99
	MicroControl	Completed	4-132

INDEX OF PRODUCTS BY TYPE

I. UNIX-like Systems:

II. Proprietary Systems:

Vendor	Product/Product Type	Evaluation Status	Page
Computer Associates International			
	ACF2/MVS	Completed	4-104
	acf2/VM	Completed	4-69
	Top Secret	Completed	4-106
Concurrent Computer Corporation			
	OS-32 real-time operating system	DA	4-32
Control Data Corporation	NOS	Completed	4-60
Data General Corp	AOS/VS	Completed	4-79
Digital Equipment Corporation			
	VAX/VMS 4.3	Completed	4-62
	SE-VMS	DA	4-32
Gemini Computers, Inc.	GEMSOS	DA	4-32
	M-Component	DA	4-32
Hewlett Packard Computer Systems Div.			
	MPE V/E	Completed	4-77
Honeywell Information Systems, Inc.			
	Multics	Completed	4-58
	SCOMP	Completed	4-56
International Business Machines Corp			
	MVS/RACF	Completed	4-102
	MVS/XA with RACF	Completed	4-72
	VM/SP with RACF	Completed	4-88
	MVS-ESA/RACF	Completed	4-95
	VM/SP	DA	4-32
Prime Computer, Inc.	Primos	Completed	4-75
Tandem Computers Inc.	Guardian-90	DA	4-32
Unisys Corp.	A Series	Completed	4-67
	OS 1100	Completed	4-85

Vendor	Product/Product Type	Evaluation Status	Page
Wang Laboratories, Inc.	SVS/OS	Completed	4-99

III. Networks and Network Components:

Vendor	Product/Product Type	Evaluation Status	Page
Amdahl Corp.	Network Component	VAP	4-30
Boeing Aerospace	SNS SNS + NM	Formal	4-44
Verdix Corp.	VSLAN	Completed	4-91

IV. Subsystems:

Vendor	Product	Page
ALC Stealth Group	Tigersafe	4-128
ALC Stealth Group	Tigersafe Ver 3.03.01 EN	4-137
Clyde Digital Systems	Dialback	4-123
Codercard, Inc.	CPP-300	4-111
Computer Accessories, Inc.	Private Access	4-122
Computer Security Corp.	Citadel	4-124
Computer Security Corp.	Sentinel	4-116
Cortana Systems Corp.	PC Security	4-120
Enigma Logic., Inc.	Safeword	4-115
Eyedentify Inc.	EIS	4-139
Fischer International	Watchdog	4-112
Fischer International	Watchdog Armor	4-141
Gordian Systems, Inc.	Access Key	4-110
IDENTIX Corp.	IDX-50	4-119
Infosafe Corp.	X-LOCK-50	4-125
Infotron	INX 4400	4-126
Key Concepts, Inc.	SureKey	4-118
Micronyx, Inc.	Triad Plus	4-117
	TriSpan	4-130
Pyramid Development Corp.	PC/DACS	4-134
Security Dynamics, Inc.	ACE	4-114
Spectrum Manufacturing, Inc.	DPS 800/12	4-124
Sytek, Inc.	PFX Passport	4-113
United Software Security	OnGuard	4-136
Wang Laboratories	MicroControl	4-132

VENDOR ASSISTANCE PHASE

POTENTIAL PRODUCTS LIST

I. Trusted Systems and Operating Systems (UNIX-like Systems)

Vendor	POC & #	Product Description
Amdahl Corporation	Bill O'Connell (408)746-6891	Unix based Operating System
Convex Computer Corp	Blair Baker (214)497-4536	Unix based Operating System
Harris Corporation	Wendell Norton (305)973-5201	Unix based Operating System
Silicon Graphics Inc	Linda Jo Dolny (415)335-1021	Unix based Operating System
Deleted April 91 ~~Sun Microsystems~~	~~Larry Baron (408) 276-3414~~	~~Unix based Operating System~~
Cray Research, Inc.	Paul Falde (612) 683-5467	Unix based Operating System

II. Trusted Systems and Operating Systems (Proprietary Systems)

Vendor	POC & #	Product Description
None		

III. Network Systems and Network Components

Vendor	POC & #	Product Description
Amdahl Corporation	Bill O'Connel (408)746-6891	Network Component
Loral Command and Control	Larry Megalo (719) 594-1012	Network Component

VENDOR ASSISTANCE PHASE

POTENTIAL EVALUATED PRODUCTS LIST

I. Trusted Systems and Operating Systems (UNIX-like Systems)

Vendor	POC & #	Product and Candidate Division
Addamax Corp.	Randall J. Sandone (217) 359-0700	System V UNIX System - B 4.3BSD UNIX System - B Compartmented Mode Workstation - B
AT&T	Jeanne M. Baccash (201) 522-6028	UNIX V - B
Digital Equipment Corporation	Paul T. Cummings (508) 264-5026	Compartmented Mode Workstation - B
Sun Microsystems	Larry Baron (408) 276-3414	Compartmented Mode Workstation - B

II. Trusted Systems and Operating Systems (Proprietary Systems)

Vendor	POC & #	Product Description
Concurrent Computer Corporation	Chris J. Kirschman, Jr. (201) 758-7566	OS-32 real-time operating system - C
Digital Equipment Corporation	Barney Loiter (301) 731-3717	Security Enhanced VMS - C/B
Gemini Computers Inc.	Dr. Tien F. Tao (408) 373-8500	GEMSOS-A M-Component - A
International Business Machines Corp	David M. Frayne (914)288-2612	VM/SP-C/B
Tandem Computers Inc.	William J. Buer (408) 725-6000	Guardian-90 - C

APPENDIX C

SECURE NETWORKING PRODUCT SUMMARY

TABLE C-1. CATEGORIES OF NETWORKING PRODUCTS

CATEGORY A (Based on trusted software without Type 1 encryption)	CATEGORY B (Based on Type 1 encryption without trusted software)	CATEGORY C (Based on both Type 1 encryption and trusted software)	CATEGORY D (Based on neither Type 1 encryption nor trusted software)
• Verdix VSLAN	• Xerox XEU	• BLACKER	• Commercial Gateways and Routers
• Boeing MLS LAN	• Motorola NES	• CANEWARE	• Commercial LANs (Ethernet, FDDI)
• Loral MLS-100 Gateway	• Wang TIU		• Intelligent switches (X.25, T-1)
• Gemini Trusted Network Processor	• KG-xxx		• Products based on DES encryption
• HFS XTS-200 used as Guard or Switch			• Network Operations Center products
• Amdahl Multiple Domain Facility			

TABLE C-2. SUMMARY OF PRODUCT FUNCTION AND CERTIFICATION STATUS

Product Identification	Certification Status	Product Function
Verdix VSLAN	EPL B2 Completed	MLS Ethernet LAN components including secure router for interface to KGs, BLACKER, or Caneware.
Boeing MLS LAN	EPL A1 Formal Evaluation	MLS Ethernet LAN based on Secure Network Servers. Router under development. Interoperable with BFE/CFE?
Loral MLS-100 Gateway	EPL B2 Vendor Assistance	MLS gateway/guard/multiplexer with X.25, BLACKER, Internet, serial and Ethernet interfaces.
Gemini Trusted Network Processor	EPL A1 Design Analysis	Trusted network processor based on GEMSOS security kernel.
HFSI XTS-200	EPL B3 Formal Evaluation	MLS processor with UNIX-like operating system; can be configured as an intelligent switch or network guard.
Amdahl Multiple Domain Facility	EPL B2 Vendor Assistance	Hardware/software components which partitions Amdahl mainframe (running B2 Unix) into as many as14 domains
Xerox XEU	ECPL Type 1	Acts as bridge between processor it serves and Ethernet. Inserted in-line on transceiver cable.

TABLE C-2. SUMMARY OF PRODUCT FUNCTION AND CERTIFICATION STATUS (CONT)

Product Identification	Certification Status	Product Function
Motorola NES	ECPL Type 1	SDNS compatible front end/gateway for single level host or network. Ethernet, X.25, and CANEWARE compatible.
Wang TIU	In process for Type 1	Acts as bridge between processor it serves and Ethernet. Inserted in-line on transceiver cable.
KG-xxx	ECPL Type 1	Various models for bulk encryption of point-to-point WAN trunks.
BLACKER Front End (KI-111)	Designed for A1 and Type 1	MLS packet encryptor used as DDN interface for host or network gateway; GOSIP migration planned; 64Kbps
CANEWARE Front End (AN/CYZ-21)	Designed for B2 and Type 1	MLS network interface compatible with SDNS, T1 and BLACKER.

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
UNISYS/ TIMPLEX Secure FDDI	FDDI 802.3 TOKEN Ring X.25 RS-232 RS-449 V.35	IP XNS IPX	SNMP MIB BER	SAC Accredited at C2 Moving to B1 Accreditation	Meets DNSIX security -B1 Installation Base in INTEL Communities	Supports OSI Each Concetrator supports 32 single Stations Each FDDI Adapter provides 12 ports per unit for WAN Interface	N/A	Serial link rate of 2.048MB/Sec per Port Supports Dual Ring FDDI backbone at 100MB/Sec per ring	Lorraine Martin 805-987-9445
VERDIX SLAN	802.3	TCP/IP	SNMP	EPL-B2 MDIA	Consistency of Labeling in Heterogeneous Enviornment	Could move to COSIP 128 NODES FDDI	UNIX VMS VLTRIX DOS A/UX XENIX	Serial link rate of 2.048MB/Sec per Port Supports Dual Ring FDDI backbone at 100MB/Sec per ring	Gary Bowles 703-378-7600
IP Router	802.3	TCP/IP	SNMP	Submit Documentation 3rd Quarter for B2	Secure IP Routing	Ready to move to COSIP 1000 NODES	N/A		

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
Boeing MLS LAN	802.3 VME DR-11 Analog/Video (Separate Cable) RS-232	TCP/IP	SNMP next year	Awaiting Technical Review Board for A1	Simultaneous Multilevel secure comm.	No Trunk Encription between services Plans for OSI and GOSIP No VMSOS 254 servers per network 3200 devices per network	UNIX VLTRIX	235KB/Sec end to end (TCP) 420 KB/Sec end to end UDP	Ken Takevchi 206-773-0628
LORAL Multinet Gateway MLS-100	802.3 x.25 ARPANET DDN X.25 Blacker X.25	IP Datagram	N/A	Expected on EPL during of summer of 92	IP Gateway/ Switch	Need to recode for GOSIP Not a Router	N/A	56KB/Sec 250KB/Sec	Erv Perelstein 719-594-1129

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
GEMINI Trusted Network Processor	802.3 X.25 RS-232	Lower layers of OSI and DOD supported	NONE	Moving toward Formal Evaluation for A1	Verified Design Based on UNIX Sys 5	Interface to higher layers must be user developed Uses DES Algorithm No Network Mgnt Interface Limited X.25 Channel capability	UNIX for sys develop ment envlorn ment	1MB/Sec 802.3 19-15 KB/Sec X.25 RS-232 up to 64 channels	Mike Thompson 408-373-8500
OTHERS									
Motorola BLACKER & Network Encryption Unit									Jerry Hogg 602-441-2628 Vicki Beseke 602-441-3232
XEROX XEU									Frank Presson 703-442-6777
Digital DESNC									Bruce Pacot 719-260-3311
Digital One Way Gateway									
WANG Trusted LAN I/F Unit									Powell Glenn 508-967-8699

APPENDIX D

WAN PRODUCT DATA

Characteristics

Product History

Models: IDNX/10, IDNX/20, IDNX/40, IDNX/70, IDNX/70T, and IDNX/90.

Date of First Delivery: IDNX/40—September 19, 1986; IDNX/70—October 10, 1986; IDNX/20—December 1, 1987; IDNX/10—December 1989; IDNX/90—September 1990; ADNX/48—scheduled for the end of 1990.

Number Installed to Date: 3,423 IDNX nodes shipped as of July 1, 1990.

Description

The **IDNX/10** supports one active and one redundant T1 trunk. A single T1 line on an IDNX/10 supports up to 23 voice circuits or 30 data circuits.

Each **IDNX/20** node can terminate up to 15 T1 trunks and support up to 336 active voice circuits or 84 active data circuits at 1.2K bps to 19.2K bps or 56 active data circuits at 56K bps. The maximum aggregate data rate is 1.344M bps.

An **IDNX/40** node can terminate up to 15 T1 trunks and supports termination/origination of up to 68 active data circuits. Up to 512 pass-through voice/data circuits are supported.

An eight-shelf **IDNX/70** node can terminate up to 96 T1 trunks. It supports up to 1,024 active voice/data circuits per node, either on a demand-assigned or permanent basis.

The **IDNX/90** supports up to four T3 connections. Each T3 trunk module provides connection for a single T3 circuit.

IDNX features include preempted priority assignment; support for cable, microwave, satellite, and fiber optic media; time-of-day bandwidth reservation; demand-assigned bandwidth; and selectable call routing attributes, including terrestrial/satellite, encrypted/nonencrypted, and CCITT ADPCM/N.E.T. ADPCM/ADPCM plus 8K bps and 16K bps Vector Adaptive Predictive Coding compression.

Network clocking and synchronization are accomplished through a choice of internal or up to eight external clocking sources with a fallback priority scheme. The IDNX internal oscillator meets stratum 3 accuracy criteria. Pass-through timing is supported when the network is locked to a different frequency from the data circuit.

The IDNX supports centralized and/or distributed integral network control and management. Capabilities include password protection and operator privilege levels, network monitoring, diagnostics, and reconfiguration. Diagnostics include comprehensive loopback tests. Extensive parameter selection is available. For example, call processing parameters configurable from the operator console include Maximum Calls on Node (1,024 maximum); Maximum Call Setup Retries (1 to 4); Maximum Hops per Call (1 to 12); Maximum Satellite Hops; Call Statistics Reporting Interval (1 to 1,440 minutes); Call Detail Recording Enable/Disable; Reconnect Timeout (1 to 60 seconds); Pre-empt Control (0 to 11, indicating the maximum number of hops that a preempted priority call can take to reach its destination without preempting other calls); and Number of Links to Node.

ADNX/48

The Access Digital Network Exchange (ADNX/48) Integrated Access Managers are intelligent channel banks that complement the IDNX family. The ADNX/48 is designed for local applications where more than 12 voice circuits require connection to an IDNX, but where a direct digital PBX connection is unavailable. The ADNX/48 also provides access for sites that require connection to the public network for voice circuits as well as high-speed access to a private backbone network for LAN connections or video- or teleconferencing equipment. The ADNX/48 especially complements the IDNX/10, which is best used in small, data-only, remote applications.

The ADNX/48 is suited for drop-and-insert applications, multidrop applications, and applications that usually would require two channel banks. Software controls provide configuration and fault management tools to meet the requirements of remote sites.

The ADNX/48 permits flexible configuration options. It can perform dual T1 operations (up to 48 channels); single T1 operation (24 DS0 channels); and bidirectional, drop-and-insert operation.

The following software-programmable voice cards are part of the ADNX/48:

- DS1 digital PBX interface
- 4-wire E&M/PLR/TO (Terminate Only)
- 2-wire FXS/DPT/PLAR Megacomm
- 2-wire FXO/DPO

These cards are compatible with all three ADNX/48 models.

In addition, software-programmable and hardware-configured data cards support synchronous data rates from 2.4K bps to 1.536K bps. Interfaces include V.35, RS-422, and RS-232-C. An intelligent DDS-compatible Subrate Data Multiplexing (SDM) card provides five ports per card (with a maximum rate of

9.6K bps per port). An optional integrated dual-port D4/ ESF Channel Service Unit that is compatible with all three models is available.

IDNX/10

The IDNX/10 provides connectivity to backbone networks for low-volume sites as well as compatibility with a variety of carrier services, such as fractional T1. The IDNX/10 is DS0 channelized and is fully compatible with all other IDNX products as well as with digital cross-connect systems. This allows access to such services as AT&T Megacom/800 and SDN, MCI Prism, and US Sprint VPN and Ultra WATS. Also, access to ISDN offerings will be possible as they become available.

The IDNX/10 supports two T1 trunks: one active and one redundant. A T1 facility on an IDNX/10 supports up to 23 voice circuits or 30 data circuits. Each of the IDNX/10 interface modules has a built-in channel service unit (CSU) that supports D3/D4 or extended superframe (ESF) framing patterns. This equipment accepts direct digital connection of DS1 voice; analog four-wire E&M, FXS/PLAR, and FXO; low-speed RS-232-C synchronous data; and N x 56K/64K synchronous data with V.35.

The IDNX/10 provides flexibility in configuring networks. Users with small sites can take advantage of the full array of backbone services. Furthermore, DS0 compatibility with carrier-based services lets users build hybrid networks combining public and private networks.

IDNX/10 Hardware

The Main System Shelf has five slots that can hold up to two Main Modules, two T1 Interface Modules, and one Sync 6/2 Data Module. Single or redundant power supplies are available. As an option, the user can attach the Channel Module Shelf to the Main System Shelf to extend the IDNX/10 capacity and functionality.

The Main Module contains the CPU, memory, and clocking circuitry. This module also has six I/O interfaces that accommodate local or remote connection to the Operator Interface for network management. A DS1 interface permits direct connection of a digital PBX. The module also supports an external alarm and two RS-232 data ports.

The T1 Interface Module provides a DS0 channelized trunk that is compatible with both the private and public network services, including fractional T1. An optional redundant module is available that can support redundant hardware or T1 facilities.

The optional Sync 6/2 Data Module provides connection for up to eight data ports. Two V.35 ports support speeds of up to 256K bps in increments of 56K bps or 64K bps. This module also has six RS-232-C ports for data rates up to 56K bps. The Channel Module Shelf handles high-speed data circuits, up to 1.344M bps.

The Power Supply Module distributes power to the Main System Shelf. An optional second supply can provide redundancy. Switchover is automatic if one unit fails.

The Channel Module Shelf multiplexes up to 23 channels. These can be any combination of analog voice and synchronous data. The channel module units support 4W E&M (I, II), FXS, PLAR LS/GS, and FXO voice connections. Data ports in this shelf operate in increments of 56K bps or 64K bps up to 1.344M bps with V.35 or RS-422 interfaces. RS-232-C interfaces are available.

The Power Converter/Ringer Shelf consists of a power converter module that performs AC-to-DC conversion for analog voice channel units. An additional module can be added for 1:1 redundancy. An optional Ringer Module can also be installed in this shelf to provide ringdown operation for FXS applications.

IDNX/20

The IDNX/20 manages private utility networks consisting of various types of transmission techniques, including T1. The IDNX/20 supports a maximum of 15 T1 lines. In addition, this product provides data support for the following:

- RS-232-C data at 1.2K to 19.2K bps (DCE or DTE)
- V.35 and RS-449/-422 data at 1.2K to 1.344M bps (DCE or DTE)
- Biphase data at 1.2K to 96K bps (DCE)
- DDS and M24 compatible (DSOA compatible)

The IDNX/20's AutoLoad software feature, unique to this product, automatically loads operating software from IDNX nodes in the network upon initial start-up or if a major power failure occurs. AutoLoad helps keep the cost of common equipment down by eliminating the need for resident software storage in every IDNX/20 in the network.

The Basic Operator Interface (BOI) provides diagnostics, debugging commands, and node and trunk configurations. The BOI is not AutoLoaded but is stored permanently in nonvolatile memory. Alarms are user definable and customized, and the network can be expanded without the operator having to update routing tables.

Optional equipment for the IDNX/20 includes a memory module, a T1 jackfield, and an alarm panel. The memory module provides NVRAM software storage. In a network with no IDNX/40s or IDNX/70s, at least one memory module is required per network. System software is distributed automatically by the AutoLoad function.

IDNX/20 Hardware

The IDNX/20 consists of a single-card shelf cabinet with 12 module slots, 2 of which are reserved for common logic. The IDNX/20 uses a more highly integrated technology than do the larger models, one that reduces all common logic to a single common logic board (CLB). Two versions of the IDNX/20 are available, with or without redundant common equipment. Common equipment includes one or two CLB modules, power supplies.

power distribution unit, and cooling devices. Also included is battery backup that preserves system software on the CLB in the event of a power failure. The entire unit is rack mounted or used as a standalone unit installed in an IDNX cabinet.

IDNX/20 24-Slot Version

The 24-slot version of the IDNX/20 actually offers two configurations: 12-slot and 24-slot versions. A customer whose current requirements are for a low-capacity system could install the 12-slot version and then, as needs increase, expand it to a 24-slot configuration.

Both redundant and nonredundant models are available. Modules are mounted in one- or two-card shelf cabinets that, in turn, are mounted in standard 19-inch-wide, 7-foot-high telco cabinets or in N.E.T. IDNX/40 or /70 cabinets. Each shelf holds up to 12 modules, power supplies, and a fan.

In the 12-slot model, the processor unit (the lower shelf) has 12 modules, 2 of which are reserved for common logic board (CLB) modules. With the 24-slot version, a second shelf (expansion shelf) contains an additional 12 modules, all of which can accommodate any IDNX trunk, voice port, voice compression, or data feature modules. No additional processors are required for this 24-slot version.

The CLB occupies a single shelf slot and offers two RS-232-C ports to support a locally attached or remote dial-up terminal for network management. An optional alarm panel can also connect with the CLB.

Two power supplies are needed for the 24-slot model. Two additional power supplies can be added for 1:1 redundancy.

Optional equipment includes a nonvolatile random access memory (NVRAM) module for software storage. This module is not required in the IDNX/20, because the software is automatically downloaded via the network from a neighboring IDNX/20, /40, or /70 system in the event of a power failure on the IDNX/20. A network that consists only of IDNX/20 nodes, however, does require one memory module per network. An external rack-mounted T1 jackfield can be added to provide test access to T1 trunk hardware. A rack-mounted alarm panel may be added that provides audible and visual alarm and status indicators.

IDNX/20 8-Slot Version

In January 1990, N.E.T. introduced its IDNX/20 8-slot version. This is identical to the IDNX/20 12-slot model except that its capacity is reduced by four slots to provide users with a less expensive model. Two of the eight slots are for common logic boards (CLBs), and the remaining six are available for IDNX trunk, voice, and data modules.

This product is available in redundant or nonredundant configurations. The 8-slot IDNX/20 can be configured for up to six T1 trunks (three if a redundant system). It supports a maximum of 240 active voice calls with one trunk, or a maximum of 20 active calls up to 64K bps. For any given node, the number of originating, terminating, and pass-through active calls is 1,024.

Users can upgrade an 8-slot IDNX/20 in the field by adding a 12-slot expansion shelf, thus producing a 20-slot IDNX/20. Two slots are reserved for CLBs, and the remaining eighteen can be used for network applications. The 20-slot version is available only as an 8-slot field upgrade. Both the 8-slot and the 20-slot IDNX/20s can function as stand-alone units or can be mounted in cabinets or telco racks.

IDNX/40

The IDNX/40 supports up to 15 T1 lines. It integrates voice, data, facsimile, and video bit streams over T1 networks. Nodes can be added without operators having to update or maintain routing tables. The IDNX/40 supports up to 127 voice/data channels per T1 line for efficient bandwidth utilization.

The equipment's Processor Module (CPU-2) executes the nodal software. Based on an MC68000 microprocessor, this module occupies one slot and has two RS-232-C ports. These support a local terminal and/or a modem for remote dial-in access. An optional alarm panel is also supported.

The Memory Module provides nonvolatile RAM storage for nodal software and the configuration database. New software releases can be downloaded through the network or copied from another Memory Module. At least one Memory Module is required for each IDNX/40 node. An additional module can be used to provide redundancy.

The Clock Module provides an internal timing source. The Clock Module can also use up to eight external sources for timing references, including PBXs, DDS circuits, T1 facilities, satellite controllers, or a station clock. If a clock failure occurs, the Clock Module will automatically phase lock to the next highest priority source or onto its own oscillator. At least one Clock Module is required for each node. An additional module can be used for redundancy.

The Time Slot Interchange Module (TSI-2) performs bus management, allowing modules to communicate with each other by providing time switching connectivity among modules. At least one TSI-2 module is required for each IDNX/40. An additional module can be used for redundancy.

IDNX/40 Hardware

The IDNX/40 is a dual-row, single-shelf, 24-slot node for lower capacity sites. Modules configured in the IDNX/40 are the same as those used in an IDNX/70 (see below). The IDNX/40 has 24 physical slots and 16 logical slots. The IDNX/40 can hold up to three power supplies. One or two power supplies are used to power the node, and the third can be used for redundancy.

IDNX/70

The IDNX/70's common equipment is available in a one- to four-shelf nonredundant configuration or in a one- to eight-shelf redundant configuration. The IDNX/70 is an

expandable transmission resource manager for high-capacity network implementation. It supports up to 96 T1 lines and is typically installed in headquarters or large data processing centers. An IDNX/70 can be upgraded in the field to an IDNX/90.

IDNX/70 Hardware

The IDNX/70 is a single unit mounted in one or two cabinets, with one to four shelves per cabinet and one to four power supply shelves. Two cabinets can be combined to form an eight-shelf node. Each card shelf requires one power supply, and power supply shelves can hold up to four power supplies. Thus, there is capacity for hot backup power supply units.

A card shelf is divided into a front portion and a back portion by a backplane. The module is a printed circuit board assembly consisting of a front card and a rear interface card that are connected through the backplane, on which the pins are located.

When modules are configured in the IDNX/70, two things, besides the number of physical slots, must be taken into account: the amount of available bandwidth and the power requirements of the configuration. The number of logical slots required by each module type places the first constraint on configuration. A logical slot is the measure of the backplane bandwidth requirements of a module. Each shelf has 16 physical slots and 16 logical slots. Second, any combination of modules in a shelf should not exceed a power requirement of 45 amperes. Based on this measure, it may be necessary to arrange the modules differently among the shelves.

The front cards contain the logic associated with the specific processing function performed by the module. The interface card provides the physical interface for external equipment (e.g., PBX, computer system, video equipment) to the IDNX. Ports, or access points, are located on the interface card.

IDNX/90

The IDNX/90 is designed as a platform for T3 services and high-speed applications that require multimegabit transmission. In a March 1988 position paper entitled "T3 Statement of Direction," N.E.T. explained that "in a non-subrated DS-3 format, the signal can take whatever format is required by the application, the only requirement being that proper framing be maintained." (N.E.T. expects to provide channelized, subrated T3 in the future.) The new IDNX/90 is designed to accommodate existing IDNX modules. In addition, it is fully compatible with the IDNX/70, IDNX/40, and IDNX/20 resource managers; the IDNX/10 Integrated Access Multiplexer; and the company's complete line of network management products. Customers can upgrade an IDNX/70 to an IDNX/90 in the field.

The IDNX/90 uses the Motorola 68030 high-performance microprocessor; it provides a 256M bps, nonblocking, switching architecture. The T3 trunk module provides support for IDNX internodal trunks operating over nonsubrate T3 facilities. This module can allow such networking applications as LAN interconnectivity, host-to-host communications, distributed graphics, and supercomputer networking.

The IDNX/90 supports up to four T3 connections; each T3 trunk module provides connection for a single T3 circuit. The module can be configured for 1:1 redundancy so that, if the IDNX/90 detects a fault, it can automatically switch traffic to the redundant module.

IDNX Modules

The IDNX supports four types of modules: control modules, T1/E1/64K bps/56K bps trunk modules, port modules, and server modules. The functions of these modules are described below.

Control Modules

Control modules control or manage the IDNX internal logic. They are the common equipment modules and are required in each IDNX. The control modules include processor and memory, TSI-2, and clock modules.

Processor and Memory Modules

The processor module, which controls and runs the system software, consists of a front CPU card and a rear interface card. The front card is called the CPU-2, while the CPU cards in earlier releases were known as CPUA. The rear interface card is known as the Input/output processor (IOP). The front card contains a Motorola 68000 microprocessor, system control logic, and RAM.

The interface card has two RS-232-C asynchronous ports. The operator console uses one port to access the operator interface. The second port is typically used for connection to an auto answer modem for remote diagnostic access, as an additional operator console, or as a printer port to record events.

At least one processor module and one memory module must be installed in each node (or two each for redundancy). Additional processor modules can be installed to create a multiprocessor environment on a node to handle large amounts of voice and data traffic. When two or more processor modules are used, one is the master and the others operate as co-processors sharing the IDNX work load. When the master fails, a co-processor becomes the master. The operator interface determines which processor module functions as the master, indicated by the lights on the card's front panel. One memory module can support any number of processor modules on a single node.

TSI-2 Modules

The time slot interchange modules control information switching through the CPU-2 processor modules and other cards on the node by means of the transport bus. Nodes supporting CPUA (software prior to Release 6) run with TSI. Both TSI and TSI-2 provide the same functionality. TSI-2, however, provides for redundancy where TSI does not. The TSI module uses a multiplexer interface card. This is the only module that must be in each shelf and must be in an assigned slot. For redundancy, a second TSI module can be installed on each

shelf. The second TSI module must be installed in the slot next to the primary TSI module. Most CPUA and TSI modules in the field have by now been upgraded.

Clock Module

The clock module serves as an internal timing source and can be used to synchronize an entire network. This is accomplished by phase-locking to the appropriate reference derived from ports, trunks, or the internal oscillator on the clock module itself. The clock module can accept a timing reference from any one DS1, PRI, PRC, INTL, 56K TRK, 64K TRK, TMCP, NXTK, and all RS-422 trunk modules as well as universal synchronous data modules. All shelves in the cabinet receive timing from the clock module. This module performs ongoing internal tests to monitor the eight clocks it generates.

The CLK-2 card provides stratum 3 accuracy. With Release 6 and later CLK-2 cards, the offline card can be inserted and removed without interfering with the primary card by repositioning the switch on the front of the card. There must be at least one clock module in each node. A second clock module can be installed through the operator interface for reliability. When the IDNX switches to the redundant clock module, the node restarts. During a power-up condition, the modules determine which clock module is active.

IDNX/20 CLB Module

The CLB module incorporates CPU, time slot interchange (TSI), and clock functions. It is based on a Motorola 68000 microprocessor. Resident memory includes EPROM for the Basic Operator Interface (BOI) and AutoLoad feature, RAM for system software storage and execution, and nonvolatile RAM (NVRAM) for the configuration database. The CLB occupies a single slot in the IDNX/20 cabinet. Two RS-232-C ports are available to support locally attached or remote dial-up terminals for network management. A connector on the CLB is also provided for an interface to an optional alarm panel.

Clocking functions, contained in the CLB, serve as an internal timing source for synchronizing the node. The CLB also performs bus management and time slot interchange functions which provide connectivity among modules contained in the IDNX/20.

Trunk Modules

Trunk modules contain logic to control the flow of information into the T1 facilities. The trunk module is the point at which a call (either voice or data) leaves the node (IDNX) and enters the network or arrives from a remote node. A call is the virtual port-to-port circuit built by the supervisor software. Trunk modules function as frame builders and work in conjunction with the processor module to allocate and deallocate trunk channels. The modules contain realtime multiplexing, synchronization, and control logic, and they support standard Red and Yellow alarms. The nine trunk modules are the IDNX T1 trunk, MIL-188, RS-422, CEPT, 56K, CMIT, NXTK, International 422, and 64K.

T1 Trunk Module

The T1 trunk module supports one T1 trunk (1.544M bps). It functions as the frame builder and works in con junction with the processor module to allocate and dea locate trunk channels. The module contains realtime multiplexing, synchronization, and control logic and supports standard Red and Yellow alarms. For one-to-one redundancy, a backup trunk module can be installed. Redundancy is accomplished through hardwar cabling and through a trunk parameter in the operator interface.

The rear interface card in the T1 trunk module is called the Bandwidth Efficient Zero Suppressing (BEZS card and provides zero suppression per Bell Publicatio 62411 (i.e., no more than 15 consecutive zeros are generated). This one insertion method requires only 2 percent (32K bps) of the T1 bandwidth. No errors are introduced by inserting ones. The speed of this card is 1.544K bps.

An alternate zero suppression method, modeled after CCITT recommendation G.922, is also provided o the BEZS interface card. This method, called Maximum Bandwidth Zero Suppression (MBZS), forces the 31st bit to 1 if there are 30 preceding zeros. This method uses no bandwidth but can introduce errors in the datastream. This method is now rarely used.

MIL-188 Trunk Module

This trunk module runs at 256K bps or 512K bps and supports encryption equipment. This module is rarely used.

RS-422 Trunk

The RS-422 trunk interface provides for data conversion between the trunk card and a synchronous high-speed serial data circuit. The interface card is backwar compatible with the MIL-188 trunk interface. The RS-422 trunk supports all the features supported by the MIL-188 trunk. In addition, it can operate at eight differ ent data speeds (256K bps, 384K bps, 512K bps, 672K bps, 1.024K bps, 1.344K bps, 1.544K bps, 2.048K bps) The speeds are set through the hardware. The interfac meets all MIL-188 specifications as well as the RS-422 specifications and supports encryption equipment.

CEPT Trunk

This interface supports the CCITT G.703/704 line encoding and framing scheme. CEPT trunk functions include data recovery, frame generation and recovery, serial-to-parallel-to-serial conversion, and timing signals. CEPT trunk speed is 2.048K bps. It supports encryption equipment.

56K Trunk

The 56K trunk module provides all IDNXs with a subra trunk that operates at 56K bps, and it can be used to back up a T1 trunk for critical circuits, as a temporary trunk while T1 facilities are being installed, as a supple mental trunk to a T1 trunk, or as a subrate trunk to a t node. The 56K interface card supports encryption but

does not support transparent signaling rates and pass-through timing from the universal synchronous data card, 24K bps compressed voice. A 56K trunk supports one 56K bps trunk line.

Coded Mark Inversion Trunk Module

The Coded Mark Inversion Trunk (CMIT) module supports the line encoding (Coded Mark Inversion) used by the high-speed digital networks of Japan. The standard 1.544M bps line speed is supported by the CMIT module and lets the user properly frame data at four speeds: 192K bps, 384K bps, 768K bps, and 1.536M bps. This module provides the same functionality as the T1 trunk module, including internodal signaling and support for voice compression.

1.920-X.21 Trunk (NXTX) Module

The NXTX Trunk module supports internodal trunks that operate through 1.920M bps trunk facilities, such as Transfix in France. The interface is compatible with X.21 electrical and physical standards.

International RS-422 Trunk Module

The INT422 Trunk module is intended for those applications that require support for narrower bandwidth applications, such as 128K bps and 192K bps. N.E.T. has found that clients usually do not distinguish between international and other RS-422 applications.

The INT422 Trunk module operates at the following eight rates: 128K bps, 192K bps, 256K bps, 384K bps, 512K bps, 768K bps, 1.536K bps, and 1.544K bps bps. This list includes three new rates: 128K bps, 192K bps, and 1.536K bps. The rates of 1.024K bps, 1.344K bps, and 2.048K bps will continue to be supported in the current RS-422 Trunk module.

64K Trunk Module

The 64K is a new trunk module that supports both an X.21 and a V.35 interface. This operates as a low-speed trunk or as a backup to critical higher speed circuits.

Port Modules

Port modules connect external equipment (e.g., PBX, computer system, terminal, statistical multiplexer, video equipment, etc.) to the IDNX. There are two types of modules: data and voice.

Data Port Modules

Data port modules manage the interface between synchronous data devices (e.g., modem, front-end processor, statistical multiplexer, host computer port, etc.) and the IDNX. Data port modules are divided into three groups: low-speed, high-speed, and universal synchronous data. Each data port module supports remote and local loop via switch, signal, or the operator interface. Redundant data cards are not installed on the node. Extra data cards can be purchased for replacement upon failure of a data card on the node. Table 1 lists the speeds for the IDNX data port modules. Table 2 lists the ports and interfaces.

DS0A Module: The DS0A module provides four independent, synchronous data ports with RS-232-C DCE or DTE interfaces at rates from 2.4K bps to 64K bps and incorporates 32 bits of buffering for long-haul and multi-polling tail circuits. It transports synchronous data between IDNX and DDS networks and is compatible with the Dataphone Digital Service (DDS) specifications. The DS0A module allows data to be passed between a data terminal (DTE or DCE) and a 64K bps DS0 channel on a primary rate card in a permanent circuit.

Quad Synchronous Data Module: The Quad Synchronous Data (QSD-2) module provides four independent, rate-selectable, half- or full-duplex synchronous circuits and is configured as a data communications equipment (DCE) or a data terminal equipment (DTE) electrical interface. Rates from 1.2K bps to 19.2K bps support the RS-232 DCE or DTE interface. Rates from 1.2K bps to 56K bps support the V.35 DCE or DTE interface.

Quad Asynchronous/Synchronous Data Module: The QASD module provides 4 independent asynchronous/synchronous data ports with V.35 DCE/DTE or RS-232 DCE/DTE interfaces. The DCE interface cards provide transmit and receive timing from external DCE. Optional Terminal Timing (TT) can be used, depending on the application. This compensates for phase shifts in Send Data relative to Send Timing signals. TT is often justified with tail circuit modems, high bit rates, long cable runs, or certain other terminal equipment requirements. TT is supported on both the DCE and DTE interfaces.

High-Speed Synchronous Data Module: The high-speed synchronous data (HSD) module supports two independent, rate-selectable, full-duplex circuits with V.35 DCE/DTE or RS-422 DCE/DTE interfaces at rates from 9.6K bps to 1.344M bps and RS-232-C DCE/DTE interfaces at rates from 1.2K bps to 19.2K bps. The module requires from one fourth to two full logical slots, depending on the speed selected.

High-Speed Data Module: The HSD-2 module is a superset of the HSD module. Each HSD-2 module port operates in either emulation mode (in which it emulates the HSD module) or native mode. In native mode the ports can support N × 56K bps or N × 64K bps data rates up to 1.544M bps. In native mode connections can be made to the PRC module. This feature lets calls be placed between the IDNX/10 high-speed data ports and the HSD-2 module ports.

Universal Synchronous Data Module: The universal synchronous data (USD) module provides two independent, rate-selectable, full-duplex circuits with V.35 DCE/DTE or RS-422 DCE/DTE interfaces at rates from 1.2K bps to 1.344M bps and RS-232-C DCE/DTE interfaces at rates from 1.2K bps to 19.2K bps. The module also supports biphase DCE interface at rates of 1.2K bps to 96K bps (through a hardware DIP switch). The electrical interface is MIL-188. The biphase interface provides Manchester encoding that allows clock information to

Table 1. Data Rates Available for IDNX Data Port Modules (in bps)

			QASD					
USD	**HSD**	**QSD-2**	**Sync**	**Async**	**DSOA**	**DMD**	**QXP**	**HSD-2**
1200	9600	1200	1200	75	1200	1200	1200	144.0K
1800	12.8K	1800	1800	150	2400	1800	1800	153.6K
2400	19.2K	2400	2400	300	4800	2400	3600	234.0K
3200	32.0K	3600	3600	600	8000	3600	7200	336.0K
3600	38.4K	4800	4800	1200	9600	4800	14.4K	672.0K
4800	48.0K	7200	7200	1800	16.0K	7200	16.0K	1.152M
6400	56.0K	9600	9600	2400	32.0K	9600	19.2K	1.536M
7200	57.6K	14.4K	12.0K	3600	56.0K	14.4K	28.8K	1.544M
8000	64.0K	16.0K	12.8K	4800	64.0K	16.0K	32.0K	
9600	72.0K	19.2K	14.4K	7200		19.2K	38.4K	
12.8K	96.0K	28.0K	16.0K	9600		28.8K	56.0K	
14.4K	112.0K	32.0K	16.8K	14.4K		32.0K	64.0K	
16.0K	115.2K	38.4K	19.2K	16.0K		38.4K		
16.8K	128.0K	48.0K	24.0K	19.2K		48.0K		
19.2K	168.0K	56.0K	28.0K			56.0K		
24.0K	192.0K		32.0K					
28.8K	224.0K		38.4K					
32.0K	230.4K		48.0K					
38.4K	256.0K		56.0K					
48.0K	384.0K		57.6K					
56.0K	448.0K		64.0K					
57.6K	512.0K							
64.0K	768.0K							
72.0K	896.0K							
76.8K	1.024M							
84.0K	1.344M							
96.0K								
112.0K								
115.2K								
128.0K								
144.0K								
168.0K								
192.0K								
224.0K								
230.4K								
256.0K								
288.0K								
336.0K								
384.0K								
448.0K								
512.0K								
102.4M								
134.4M								

Table 2. Port and Interfaces

	USD	HSD	QSD-2/QASD	DSOA	DMD	QXP
No. of Ports	2	2	4	4	4 external 4 internal	4
Interfaces						
DCE	RS-232-C RS-449/-422 V.35 Biphase	RS-232-C RS-449/-422 V.35	RS-232-C V.35	RS-232-C V.35	RS-232-C V.35	X.21
DTE	RS-232-C RS-449/-422 V.35	RS-232-C RS-449/-422 V.35	RS-232-C V.54 V.35	RS-232-C V.35	RS-232-C V.54	X.21

be imbedded into and recovered from the datastream. The module requires from one fourth to two full logical slots, depending on the rate selected.

A data port configured as DTE on the universal synchronous data module can be used as a network timing source. It also allows data circuits to run asynchronously to the network clock and accommodates special signaling requirements. Pass-through timing, not locked to the internal IDNX network clock, allows an independently synchronized data circuit to be passed through the IDNX without data loss due to a frequency slippage.

Digital Multidrop Data (DMD) Module: The Digital Multidrop Data (DMD) module connects multiple terminals to a single data channel in the network. It offers four external ports for local or tail circuit connections to terminals or terminal controllers and four internal ports for network connections. Three of these internal ports permit cascaded configurations of multiple DMD modules in the IDNX network. The fourth internal port (Port 0) provides the link between the front-end processor and all other ports on the module. The external ports can be either looped in, toward the network, or out, toward the terminal. The DMD performs automatic loop testing on each external port during power-up procedures or upon getting an operator command. When the test is completed, the external ports are restored to their original states. The DMD module supports synchronous data at speeds ranging from 1200 bps to 56K bps.

Quad X.21 Port Module: The Quad X.21 Port (QXP) module is used to interface to a leased X.21 circuit or to provide a gateway to public X.21 networks. When used in conjunction with an existing QSD-2 module, the QXP module provides X.21-to-X.21 bis interface conversion and allows devices with differing interfaces to communicate with one another.

When the QXP module is configured with a DCE interface, it can detect network loops generated by external and modem signals. This module provides four independent X.21 interfaces for data communications. It is available in both DCE and DTE versions and supports speeds from 1200 bps to 64K bps.

V.54 Support for QSD-2 and QASD Interfaces: A new rear card is offered for the QSD-2 and QASD that provides a V.54 DTE interface for standardized loop-back modem testing.

Voice Port Modules
Voice modules manage calls coming into and leaving the IDNX network.

DS1 Module: The DS1 module manages the interface between voice communications equipment (analog and digital PBXs, D3/D4 channelbanks, etc.) and the IDNX. The DS1 module has two pulse code modulation (PCM) channel groups (commonly known as *digroups*). The channel groups, each containing 24 ports, are connected to voice communications equipment. This module separates the incoming 24-channel PCM frames and recovers the A and B channel signaling bits. It accepts timing from the internal IDNX network clock, the channelbank, or the digital PBX. The module supports standard Red and Yellow alarms. N.E.T. reports that the Primary Rate module is now shipped more than the DS1 module.

Primary Rate Card Module: The Primary Rate Card (PRC) module has two modes: emulation and native. The card powers up in emulation mode, functioning exactly as does a DS1 module. In native mode, it provides all of the DS1 module features as well as ESF capabilities and diagnostics, zero suppression techniques, clear channel, clock reference settings through the software, aggregate circuits, and digroup independence. The PRC module has two PCM digroups, each containing 24 ports. In native mode, the digroups may build circuits to DS0A modules, to other PRC modules in native mode, or to DS1 modules. In emulation mode, the digroups can only build circuits to DS1 modules or PRC modules in emulation mode. The PRC module also supports unrestricted clear channels or robbed-bit signaling configurable on a per-channel basis.

The interface card provides a DS1 bipolar signal interface to two DS1 lines supporting a total of 48 ports. A backup PRC module provides one-for-one redundancy. This module accepts timing from the internal IDNX network clock, the channelbank, or the digital PBX.

Two-Megabit Channelized Port (TMCP) Module: The TMCP module is a 2.048M bps channelized port interface that accepts two G.704-formatted signals from channel banks and digital PBXs. This module is compatible with CCITT G.703, G.704, and G.732 specifications. The TMCP module can also perform gateway functions to allow devices with different formats and protocols in an IDNX network to communicate with one another. In addition, the TMCP module supports transparent signaling.

Server Module

The server module increases the trunk lines' voice call capacity by compressing the voice signal. Voice calls originate and terminate on DS1 modules, PRC modules, TMCP modules, or QAVP modules. All server modules may be used with a PRC module that is running in either emulation or native mode.

DSP Module

The digital speech processing (DSP) module provides voice call compression from 64K bps on 24 channels onto 32K bps toll-equivalent ADPCM circuits. It allows up to 47 simultaneous conversations on IDNX T1 trunks. One DSP card can handle 24 channels. Therefore, two DSP modules are required to handle the full load of a DS1 or PRC module. The module is shared on an as-required basis equally among all DS1 or PRC modules on the node. A single DSP module can provide backup for any number of active DSP modules (1:N redundancy).

Both end-to-end and intermediate voice compression are supported within a network. This requires that a DSP module be available on the origination and destination node (to compress and decompress the call), but a DSP module is not required on intermediate nodes.

A call can be designated for DSP at the origination node. If a DSP module is not available, the call is sent as PCM. When the call goes through an intermediate node that has a DSP module available, the call is compressed to DSP.

VC31 and VC62 Modules

The VC31 and VC62 modules provide the two ADPCM voice compression types: 32K bps CCITT and 24K bps N.E.T. proprietary. Mu-law and A-law sampling and compression are both supported. The VC31 module provides voice call compression from 64K bps on 31 full-duplex PCM voice circuits onto either 32K bps or 24K bps circuits. There are 32 channels in one transcoder, 1 of which is used for realtime diagnostics. The VC62 module provides voice call compression from 64K bps on 62 full-duplex PCM voice circuits onto either 32K bps or 24K bps circuits. There are 64 channels in two transcoders (32 channels each). One of the channels in each transcoder (two channels total) is used for continuous realtime diagnostics and is unavailable for use as a compression channel.

Two VC31 modules are required to support one DS1 or PRC module, and one VC62 module supports one DS1 or PRC. The module is shared on an as-required basis equally among all DS1 or PRC modules on the node. If a VC31 or VC62 module is not available when the call is originated, the call is sent as PCM. When the call goes through an intermediate node that has a VC31 or VC62 module available, the call is compressed to VC31 or VC62.

New Modules

In May 1990, N.E.T. introduced its High-Density Voice Compression (HDVC) module and the Quad Analog Voice Port (QAVP).

High-Density Voice Compression Module

The HDVC module is scheduled to be available this quarter.

The HDVC uses Vector Adaptive Predictive Coding. This module enables 8K and 16K bps compression on IDNX voice circuits. This rate of compression increases the call capacity of internodal trunks, thus maximizing current bandwidth utilization. In addition, it reduces the need for future additional bandwidth.

With the HDVC's server architecture, a single module can be shared by a number of voice ports in a node, as well as by several nodes in a network.

The HDVC module is available in two forms: the HDVC/24, which accommodates up to twenty-four 64K bps channels; and the HDVC/12, which accommodates up to twelve 64K bps channels.

The HDVC module is designed both for domestic and international applications. N.E.T. believes that, because bandwidth is relatively expensive in Europe and East Asia, the HDVC module should be especially useful in these markets.

Quad Analog Voice Port

The QAVP module is scheduled to be available this quarter.

The QAVP module provides a direct analog interface for the IDNX. This module eliminates the need for external channel banks and echo cancellers; it is useful for low-density sites requiring support for analog circuits. The QAVP module has a four-wire E&M interface and supports signaling types I through V, SSDC5A. This module is designed for both domestic and international applications.

ACS 4130

IP Router

The ACS 4130 links a TCP/IP local area network into an integrated wide-area network over both point-to-point lines and X.25 data networks. ACC's ACS 4130 IP Router meets the requirements of heavy data traffic loads by segmenting data flow into local subnets. Using dynamic routing protocols, the ACS 4130 finds the shortest path to forward a packet, and avoids delays associated with congested or failed circuits. Traffic is routed to the packet's destination, instead of through the entire network.

For DoD applications, the ACS 4130 has basic IP security options. It also provides network management using the TCP/IP Simple Network Management Protocol (SNMP). With SNMP, a user can monitor and control the internetworked topology of ACS 4130s.

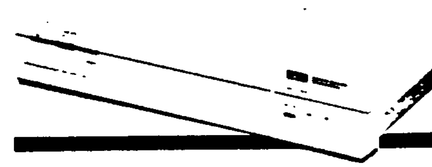
The ACS 4130 provides TCP/IP network node access across X.25 public and private data networks such as Telenet, Tymnet, Accunet, the Defense Data Network (DDN), and International Public Networks.

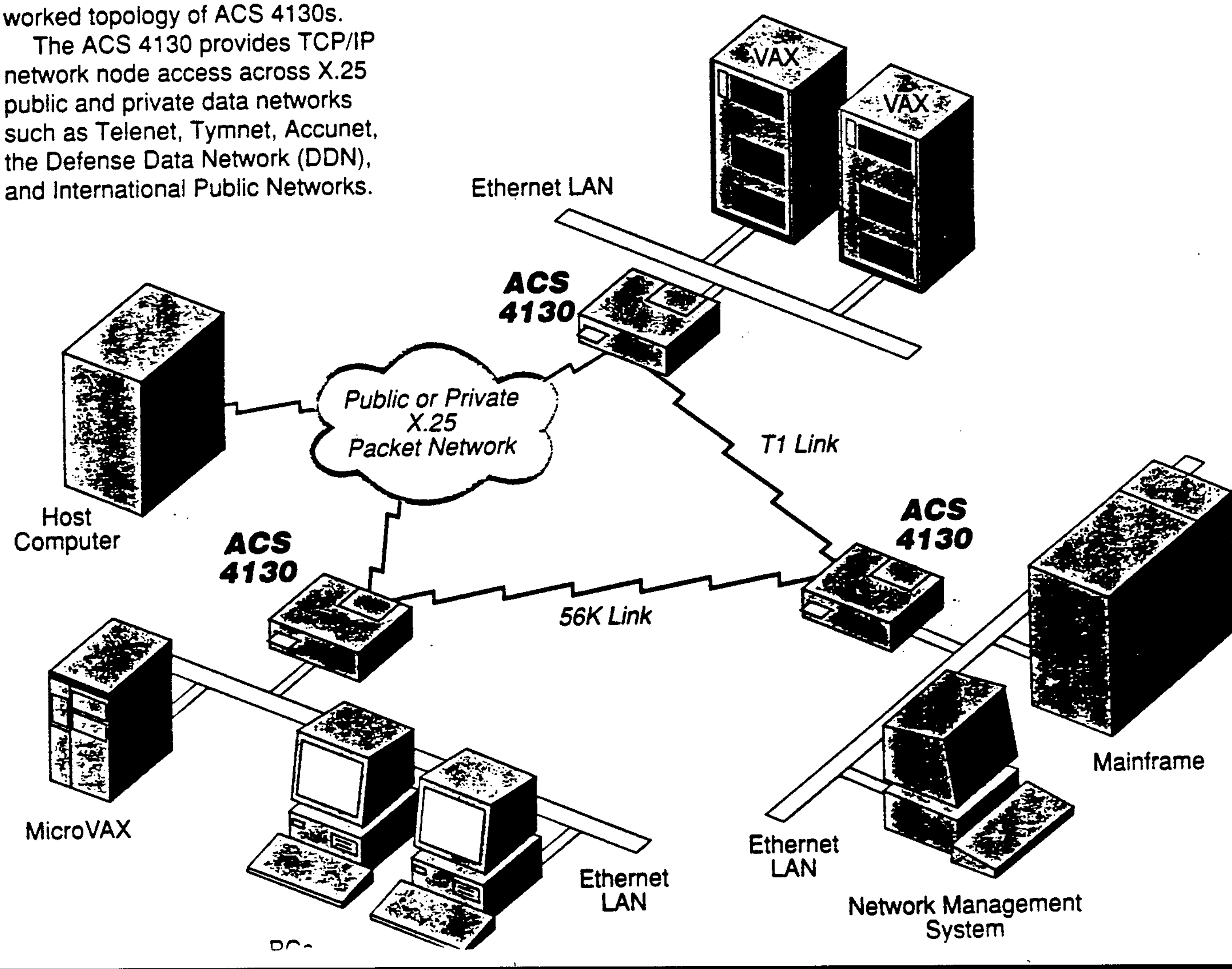
ACS 4130 Features

- Dynamic and static routing
- Subnetwork addressing
- Multiple serial ports
- SNMP network management
- X.25 support

Product Adaptability

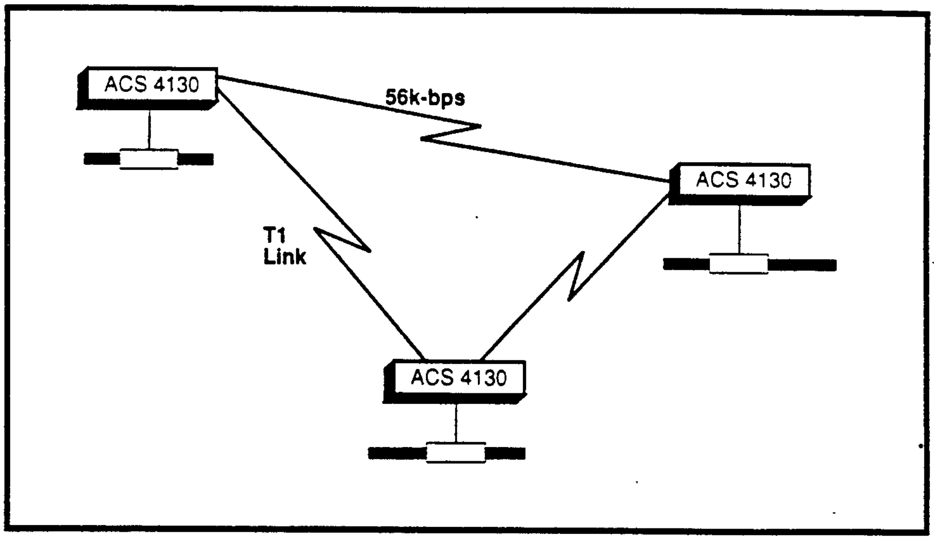
As your network changes, the ACS 4130 can take on new capabilities to keep pace with your growing requirements. All of ACC's Series 4000 advanced internetworking products share the same powerful hardware base. So different ACS 4000 bridge and router models (which are different software packages) can be interconnected in a single extended LAN.





The ACS 4130 is housed in a standalone enclosure that easily installs on your existing network. You can access system commands locally or remotely to set operating parameters, display statistics or manually set routing tables.

In today's expanding TCP/IP marketplace, the ACS 4130 provides the flexibility needed in networks with heavy data flow and multiple layers of redundancy. While both bridges and routers forward data between networks, the ACS 4130 offers significant advantages over bridges.



By evaluating the hops between the packet's current location and final destination, the ACS 4130 chooses the shortest route.

Standard Router Features

The ACS 4130 combines standard routing capabilities with second generation features to create a product with performance and flexibility that today's increasingly complex networks demand.

Dynamic IP Routing determines the optimal path to forward data.
Since the ACS 4130 IP Router operates at the Network layer of the OSI model, it examines messages specifically sent to it for routing to other networks and makes intelligent decisions about how to send packets down various paths to their proper destination. The Routing Information Protocol (RIP) analyzes the number of nodes the packet travels across to reach its destination, and chooses the shortest route.

Through RIP, the ACS 4130 discovers information about the network and shares it with other routers, sending routing updates at user-selected intervals. Once collected, the information is incorporated into routing tables.

Dynamic routing automatically accommodates network changes, keeping communication flowing.
Routing tables are configured automatically. The ACS 4130 maintains its own internal network routing tables as it receives routing updates. As it learns new network destinations, the ACS 4130 adds them to the current table automatically.

You can also customize the ACS 4130's routing tables through static routing. By manually programming routing tables, you can instruct the ACS 4130 to disregard specific packets. Through combined use of both static and dynamic routing, you maintain the benefits of dynamic routing, yet still have the overriding control of your extended network.

Subnetworks direct where packets are forwarded.
The ACS 4130 takes advantage of protocol-specific capabilities such as IP address classes and subnets. It retains separate subnetwork identities. With these, you can easily divide a set of connected networks into locally controlled administrative regions. Packets coming from one network are directly forwarded to specific subnets, and their final destination.

Advanced Features

Large interconnected TCP/IP networks create new challenges. Complex topologies spread across several sites require centralized network management and high throughput. The ACS 4130 responds to these new challenges with second generation features that guarantee high performance and continuous reliability.

Multiple serial ports provide configuration flexibility and performance options.

Multiple serial ports offer configuration flexibility. The ACS 4130 connects to either standard or thinwire 802.3 Ethernets and supports a high speed point-to-point --rial and X.25 connection. Serial ts can be any combination of RS-232, RS-422/449, RS-530, or V.35 electrical interfaces.

Multiple serial ports offer performance advantages on both large and small extended networks. On simple configurations of two Ethernets, multiple serial links can provide redundant connections and also automatically level the traffic load for continuous high throughput.

On larger topologies, multiple serial ports can be separated to connect LANs in different directions.

Multiple serial lines provide high throughput.

The ACS 4130's multiple serial lines provide aggregate speeds from 4.8 Kbits/sec up to 2.048 Mbits/sec. Serial lines from a single ACS 4130 can transmit data at different speeds. For example, one link could provide T1 capability, while the other runs at 56 Kbps into an X.25 packet-switched network.

Network Management lets you control use and operation.

A single ACS 4130 can monitor and control other ACS 4130 units on the internetwork. To indicate error alerts, it sends alarms to a user-selectable location.

ACS 4130 IP Routers function as Simple Network Management Protocol (SNMP) clients and agents, collecting data about their connected segments and reporting to network management systems that use SNMP.

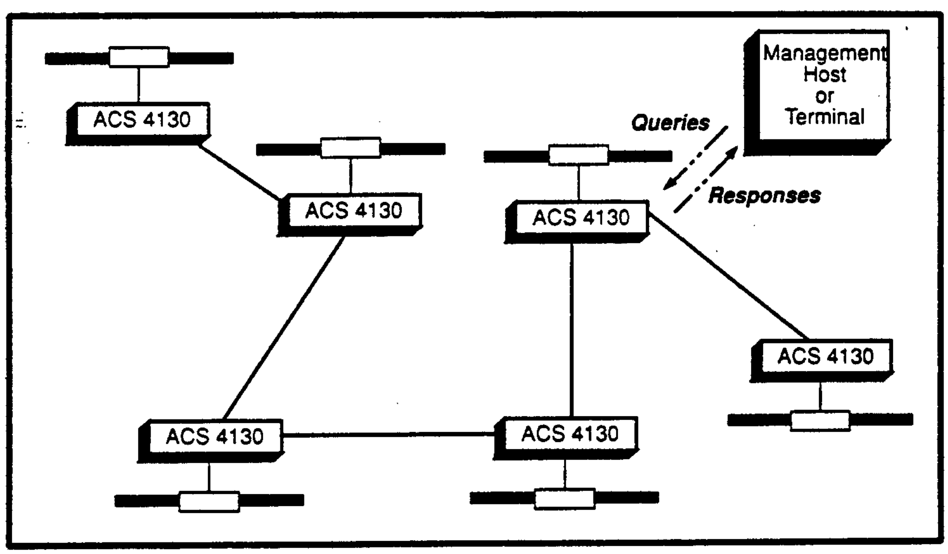
The centralized management system displays operating statistics for any ACS 4130 (or other internetworking device using SNMP) on the extended network to let you monitor network performance. It also lets you change system parameters, modify routing tables, and activate or inactivate any network links.

SNMP evolved from a need for network management that extended beyond a single LAN. With its large installed base and time-proven field performance, SNMP is the accepted standard for managing the full range of network devices.

X.25 provides network alternatives and network reliability through redundant links.

The ACS 4130 connects remote TCP/IP networks over both high-speed point-to-point and X.25 networks. An ACS 4130 can be used to link the X.25 network with remote hosts, or to interconnect other ACS 4130s through private or common X.25 carriers.

By simultaneously using point-to-point on one serial link, and X.25 on another, the ACS 4130 creates a dynamic, redundant link that serves as a backup in case of failure.



Network Management, a network administrator at a single location can query command, query status, and receive responses from any ACS 4130 in the network.

University Environment

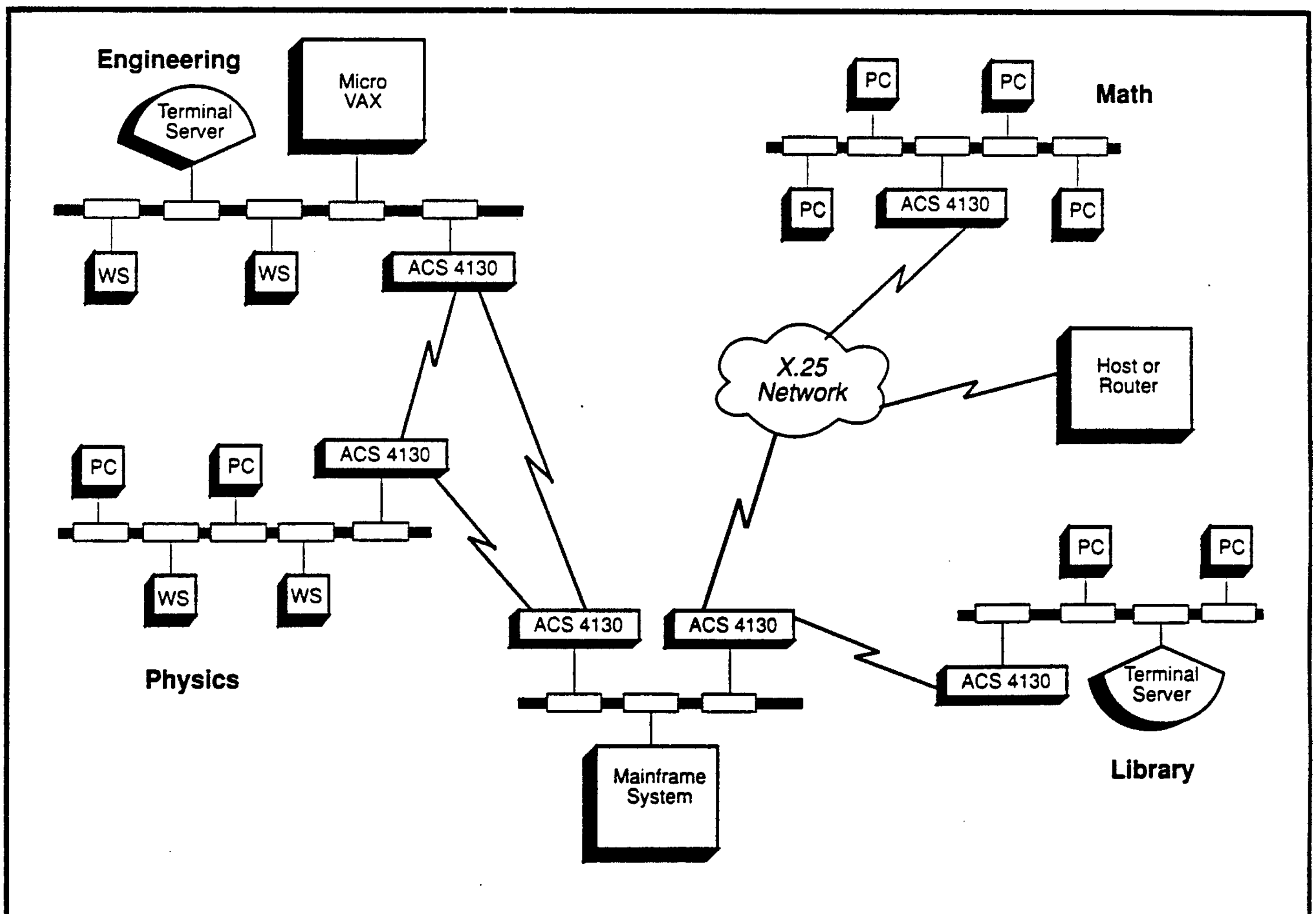
Faculty, staff, and students at one campus of a statewide university system could use ACS 4130s to give them access to resources in other departments and also to communicate with colleagues at other campuses via a regional X.25 network (i.e., CERFnet, NFSnet, NYSERnet).

Each department has at least one Ethernet LAN linking a variety of devices. The university also maintains a central mainframe system to store student records, financial accounts, and other data and applications pertinent to the entire campus. The various systems are interconnected using high-speed fiber optic lines that also carry inter-campus voice traffic.

The ACS 4130 routers could provide users with access to the mainframe resources they need. ACS 4130s would also give departmental Ethernets greater expansion options. Because with routers, individual LANs can create their own addressing scheme with no fear of duplication by devices in other departments.

ACS 4130s would also allow colleagues on separate campuses who are conducting joint research to communicate over X.25-based networks. Documents could be reviewed and returned much more quickly and with a greater degree of accuracy than any overnight mail service or even a facsimile machine could offer. Also, all the users could share one X.25 port.

Within the university environment, the ACS 4130s would use RIP packets to broadcast routing and addressing data. When a router at a departmental LAN receives a packet bound for the X.25 net, it would forward it to a router at the computer center. This router would use the External Gateway Protocol (EGP) to gather routing information from the X.25 network and forward the packet to the appropriate destination.



Manufacturing Environment

A multi-national manufacturing company can use ACS 4130 IP routers to integrate a variety of computing environments. Creating this internetwork enhances efficiency throughout the corporation. With routers, users in different corporate entities can have direct and immediate access to the information they need to do their jobs.

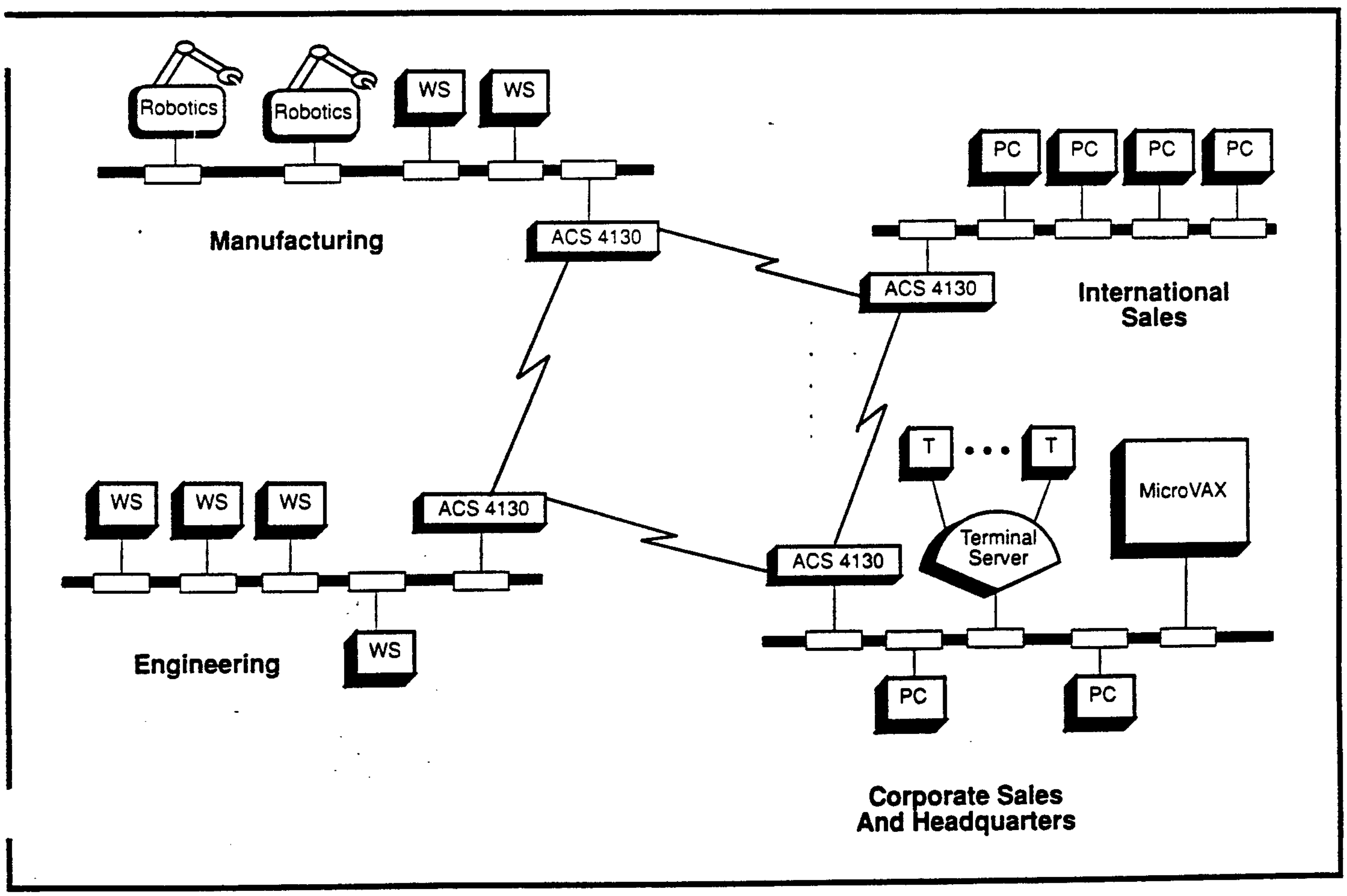
Instead of a central computer system, information system resources are distributed throughout the company. Each department chooses the hardware and software best suited to its particular needs. With the common factors of Ethernet LANs running TCP/IP, this combination of systems from many vendors could easily be linked together with ACS 4130 routers.

Since there are no connections to any public networks, the ACS 4130s would use Routing Information Protocol (RIP) to broadcast routing information to other routers in the internetwork.

Sales orders and forecasting data could be collected from international and domestic sales offices and combined into a single report for manufacturing. Because manufacturing would have information that is current and comprehensive, it could process orders more quickly and maintain inventories at optimal levels.

At headquarters, finance people could combine sales order reports and manufacturing's production schedules to prepare accounts receivables. At a separate facility, engineering could download the test procedures manufacturing needs to maintain quality control.

With ACS 4130s, the company could protect proprietary information and resources from unauthorized use. IP security could be used to prevent access to resources such as proprietary R&D information in engineering and payroll accounts in finance.



ACC Customer Service

ACC is committed to providing customers with comprehensive support and service that will help them get the most from ACC's data communications products.

Our experienced support personnel are readily available to answer your questions long after the purchase is complete.

ACS 4130 Warranty

ACS 4130 software and hardware are warranted for 90 days. After this period, ACS 4130 customers can benefit from subscribing to Service One, ACC's extended warranty plan which includes:

- Telephone Hotline. Experienced product support and technical specialists answer your questions by phone during regular business hours.
- Problem Fixes and Software Enhancements.
- Updated Software Releases and corresponding documentation.

In addition, Service One customers benefit from the ACS 4130's SNMP. Since ACC's customer service systems also support SNMP, our technicians can remotely access your ACS 4130 system to troubleshoot faults right from their desks.

Specifications

Power Requirements	***AC Voltage:*** *90 to 132 Vac, 180 to 264 Vac* ***Frequency:*** *47 to 63 Hz* ***Power Consumption:*** *100 Watts maximum*
Operating Environment	***Temperature:*** *5° to 40° C (41° to 104° F)* ***Humidity:*** *20% to 80% non-condensing*
Physical Dimensions	***Size:*** *3.5"H x 12.5"D x 17.5"W* ***Weight:*** *11 lbs.*
Serial Line Interfaces	***Two ports, any combination*** *V.35 34-pin male connectors* *RS-422/449 DB 37-pin male connectors* *RS-232 DB 25-pin male connectors* *RS-530 DB 25-pin male connectors*
Console Ports	*One male RS-232 DTE connector* *One female RS-232 DCE connector*
Network Interfaces	***One port, either option*** *Standard Ethernet (10BASE5) 802.3* *Thinwire Ethernet (10BASE2) 802.3*
RFCs Supported	*RFC 768 (UDP), RFC 791 (IP), RFC 792 (ICMP), RFC 796 (AdMap), RFC 826 (ARP), RFC 904 (EGP), RFC 950 (Subnet), RFC 1009 (Internet Gateway), RFC 1058 (RIP), RFC 1065 (SMI), RFC 1066 (MIB), and RFC 1067 (SNMP)*

ACC®

Advanced Computer Communications

720 Santa Barbara Street
Santa Barbara, CA 93101
TWX 910 334-4907
Fax (805) 962-8499
Telephone (800) 444-7854

East Coast Office
10220 Old Columbia Road
Columbia, MD 21046
Telephone (301) 290-8100

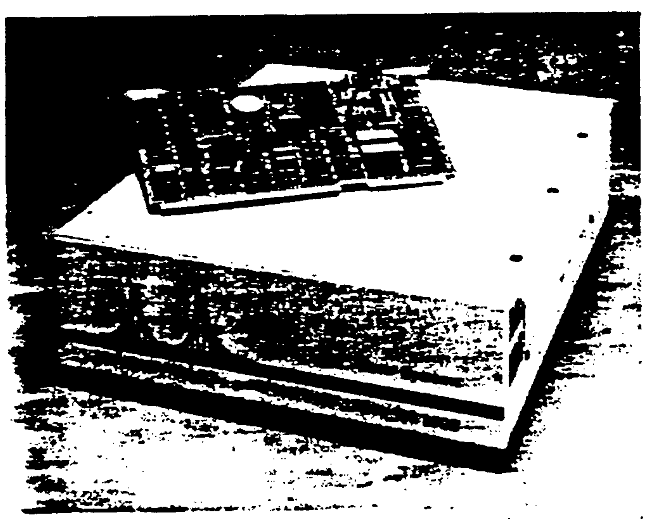
September 1989

cisco Systems Internetworking Products

datapro
ANALYSIS

Founded in 1984 by Leonard Bosack and Sandy Lerner, cisco Systems, Inc. manufactures and markets high-performance, multimedia and multiprotocol internetwork gateways and terminal servers. The company's gateway technology can be used to build wide-area networks that link an unlimited number of geographically dispersed LANs and to provide router throughput of up to 12,000 packets per second. The internetworking products of cisco facilitate the construction of large, complex, local-, and wide-area networks based on multivendor and multiprotocol computing equipment. Protocols supported by cisco products include Transmission Control Protocol/Internet Protocol (TCP/IP), X.25, DECnet, XNS, Chaosnet, and OSI. The company categorizes its product line as internetwork routers (gateways), internetwork bridge/router combinations, and terminal servers.

The cofounders of the company participated in the development and implementation of an internetwork based on the TCP/IP protocol at Stanford University, where Bosack served as Director of Computer Facilities for the Computer Science Department, and Lerner performed those tasks for the Graduate School of Business. Under Bosack's direction, Stanford became one of the first implementers of the TCP/IP standard in 1982, culminating



Cisco Systems' family of token ring internetwork routers and terminal servers are based on the firm's Token Ring Interface card, which provides a connection to token ring (IEEE 802.5) networks running at speeds up to four megabits per second.

VENDOR: cisco Systems, Inc., 1360 Willow Road, Menlo Park, California 94025. Telephone (415) 326-1941.
CANADIAN DISTRIBUTION: Granville Technologies, Toronto M5T 3A3. Telephone (416) 977-6902.
PRODUCTS: Four-member family of internetwork routers and terminal servers: Gateway Servers; STS-10 terminal server; TRouter TCP/IP terminal server and multiprotocol internetwork router; HyBridge hybrid bridge/router.
COMPETITION: Banyan Systems, Halley Systems, Honeywell Bull, 3Com, Wellfleet Communications.
PRICE: See Equipment Prices for detailed listings.

REPORT HIGHLIGHTS: **PAGE**

work begun almost two decades earlier under the sponsorship of the Defense Department's Advanced Research Projects Agency (DARPA).

TCP/IP has evolved into a mature protocol suite supported by major computer vendors and operating in many networks including ARPAnet. TCP/IP protocols are medium independent and widely implemented on commercial networks of all media types. Equipment from cisco works with all vendor TCP/IP implementations. The company is continuing to make enhancements to its TCP/IP software base.

As the basis of its internetworking technology, cisco uses the Interior Gateway Routing Protocol (IGRP), for which it has a patent pending. IGRP is a technique devised for automatic packet routing and flow optimization, which eliminates the need for static or manual routing tables that are used by other network equipment to determine routing pathways. IGRP furnishes dynamic internetwork routing, which automatically adjusts to changes in network topology or status. This technology bypasses the time-consuming, error-prone manual network tasks associated with other methods of routing. In addition, IGRP calculates in realtime within the gateway itself the following events: delay, packet type, actual traffic, error rates, and security.

cisco Systems Internetworking Products

The product strategy espoused by cisco calls for the full implementation of each of the OSI model's protocols after they are formalized by the ISO. The company's approach has always been to base its products on TCP/IP, which supports internetworking at this time and will also interoperate with ISO-specified protocols in the future. The company is also conducting research and engineering projects on Fiber Distributed Data Interface (FDDI) and ISDN.

All cisco products connect to X.25, which forms the basis for most public data networks. The products connect to Telenet, Tymnet, and AT&T's Accunet in the United States. Public data networks outside the United States accessed by cisco products include Datapac in Canada; PSS, X.25 Kilostream and Megastream in the United Kingdom; Datex-P in West Germany; and TRANSPAC in France.

This young company offers a wide selection of internetworking products, among which are gateway servers, a four-member family of internetwork routers and terminal servers: STS-10 terminal server; TRouter TCP/IP terminal server and multiprotocol internetwork router; HyBridge hybrid bridge/router; cisco Token Ring Interface; and cisco Multiport Communications Interface Board.

PRODUCT EVALUATION

One-stop shopping for all LAN needs aptly describes the product line of cisco Systems. The terminal servers from cisco can multiplex data from RS-232 serial lines and parallel I/O ports onto their high-speed network interfaces. Each terminal line supports data rates up to 38.4K bps, while providing rotary and modem functions.

PADs from cisco can furnish up to 96 devices with direct connections to public packet-switched networks or the Defense Data Networks, via X.25, X.3, X.28, and X.29 protocols. The PADs support data transfer rates to the network from 2.4K bps to 1500K bps. They also provide all the capabilities of cisco terminal servers.

The company offers Terminal Access Controllers (TACs) that can provide up to 96 devices with direct connections to the Defense Data Network via the DDN X.25 standard, DDN-DH/LH, or DDN-HDH connection methods. The TACs multiplex serial lines and parallel ports at data rates up to 38.4K bps with security on a per-line basis. The Defense Communications Agency has certified cisco TACs for attachment to the Defense Data Network.

SLIP servers from cisco can send and receive IP packets with personal computers or workstations that run under MS-DOS. SLIP software combines with cisco terminal servers to provide full-function network file transfer services to personal computers.

The terminal servers, PADs, and TACs from cisco enable users to share high-quality printers and plotters over the entire LAN.

Gateway Servers: cisco gateway servers are dynamic, high-performance, intelligent internetwork routers and gateways that send each segment of the network only those messages destined for it, a feature that avoids unnecessary traffic and eliminates broadcast storms. Users of cisco's communications and gateway servers can construct large, complex local- and wide-area networks that support internetwork communication for thousands of subnets and hundreds of thousands of host computers.

Based on the Motorola 68000 or 68020 microprocessor, cisco gateway servers support Ethernet, serial, and token-ring network channel interfaces and provide software connections through these interfaces to DDN X.25 and PSN X.25 networks. Gateways from cisco can perform in fiber optic networks because they dynamically recognize and draw upon network segments with faster transmission bandwidths. The company's gateways enable organizations to construct WANs that include major existing networks such as BITNET and CSnet (Defense Data Network), NSF regional networks such as JVNCnet and WESTnet, and public-packet switched network services such as Telenet, Tymnet, and TRANSPAC.

In April 1989, cisco announced it was offering support for Apple Computer's AppleTalk network protocol through its family of internetwork routers used exclusively in wide-area network installations. All cisco routers shipped after March will offer AppleTalk running concurrently with other protocols at no extra cost. AppleTalk routing is supported over cisco's Ethernet (IEEE 802.3), synchronous serial, token ring (IEEE 802.5), and X.25 network interfaces. The incorporation of AppleTalk into cisco's repertoire of concurrently supported protocols addresses the problem of the increasing number of Macintoshes being attached to multiple Ethernet LANs within a user installation.

Macintosh users will receive the full benefits of routers from cisco's support of AppleTalk. These routers perform network-level switching and can isolate subnetworks of Media Access Control (MAC) to protect them against noise and broadcast storms. This type of network segmentation can also overcome AppleTalk's basic limit of 254 nodes per Ethernet. Services provided by cisco's implementation of AppleTalk include Routing Table Management Protocol (RTMP), Name Binding Protocol (NBP), Echo Protocol (EP), AppleTalk Transaction Protocol (ATP), and Zone Information Protocol (ZIP).

Internetwork Routers and Terminal Servers: In this four-member family, cisco has incorporated capabilities of providing connections to token-ring (IEEE 802.5) local area networks. This new line includes a token-ring terminal server that supports up to 96 devices; a token-ring-to-

cisco Systems Internetworking Products

Ethernet (IEEE 802.3) router: a token-ring-to-token-ring router: and a token-ring-to-wide-area network router using synchronous serial lines. The four products are based on cisco's new Token Ring Interface card, which offers a connection to token-ring networks operating at speeds up to four megabits per second. Like all cisco servers, the token-ring units support multiple, concurrently running protocols, including the Department of Defense standard TCP/IP, Xerox Network Systems (XNS), Digital's DECnet, and X.25.

According to John Morgridge, cisco president, the new product line "addresses a growing corporate need to provide connectivity for entire organizations, to fully integrate the engineering networks and the PC work groups which formerly existed as islands of communication. Our new products let such organizations take full advantage of the diverse transmission media that coexist, including token-ring, Ethernet, and synchronous serial lines up to T1 speeds."

One of the principal advantages offered by the cisco routers is the elimination of the many backbone networks that users must support if they want to run multiple protocols over a wide-area network. Routers from cisco that are placed at either end of a synchronous serial backbone linking two sites let the user dispense with installing separate and costly backbones for each protocol run.

Routers can also combine network types in diverse configurations, such as connecting two token rings over an Ethernet or serial backbone, or linking a combination of Ethernets and token rings over an X.25 wide-area network.

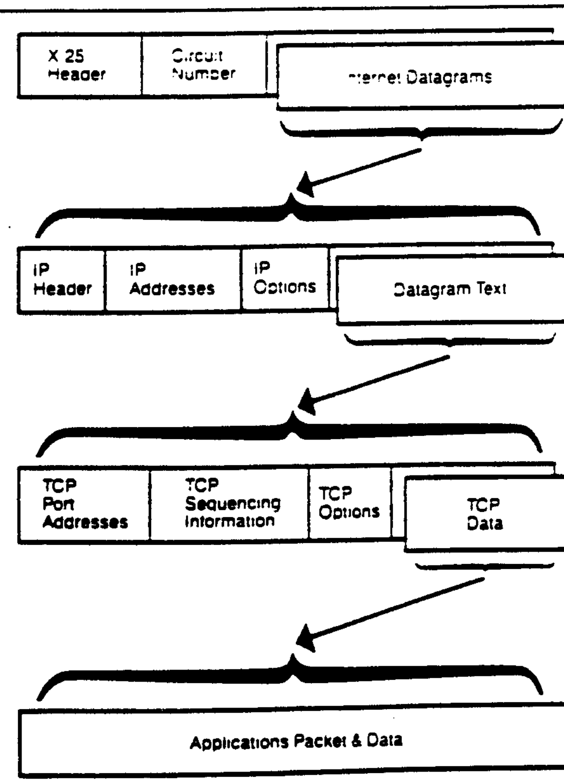
STS-10 Terminal Server: The STS-10 server provides connection for up to 10 asynchronous devices to an Ethernet (IEEE 802.3) LAN running the TCP/IP network protocol set. Placed at the low end of cisco's terminal server line, the STS-10 offers connectivity for multivendor terminals, printers, and other resources for users with geographically dispersed or departmentalized groupings. The STS-10 originated from cisco's addition of terminal server software to a hardware product purchased from Communication Machinery Corporation of Santa Barbara, California, under an OEM agreement. The multiple session feature of the STS-10 allows the terminal to open and facilitate switching among multiple remote connections.

TRouter: cisco has introduced TRouter, the first network device that combines multiprotocol internetwork routing and TCP/IP terminal service. This multifunction device addresses the needs of small work groups that require both terminal-server and packet-switching functions. TRouter provides an economical method for small- or medium-sized work groups to attain LAN or WAN access and also connectivity for modems, printers, and PCs without having to purchase a terminal server and a router. Users can place TRouter on the periphery of their networks to provide service to a remote Ethernet via a synchronous serial line at rates ranging from 9.6K bps to T1. For remote access to the network, users can attach asynchronous dial-in and dial-out modems to the serial ports. Via an X.25 data network, users can set up TRouter at a remote office to connect to other remote offices.

HyBridge: HyBridge, cisco's hybrid bridge/router, performs simultaneous bridging and routing functions on the same network. When acting as a bridge or a router, HyBridge can switch 12,000 packets per second. The chief advantage of using a multiprotocol hybrid bridge/gateway product like HyBridge is its ability to link many kinds of computers and network technologies without the use of different protocol-specific or medium-specific routers. Since HyBridge merges bridging and routing firmware, its networks provide secure and reliable gateway-based internetwork systems. In addition, the user-selectable features of HyBridge enable users to preserve their investments in LAN technology because they do not have to replace existing equipment to attain internetwork connectivity. The product offers users a growth path to large LANs and WANs.

MARKET POSITION

Responding to the need to interrelate various systems, cisco has been moving forward ever since its founding. The company has staked out a niche in the internetwork-



The TCP/IP is the de facto standard for internetworking

APPENDIX E

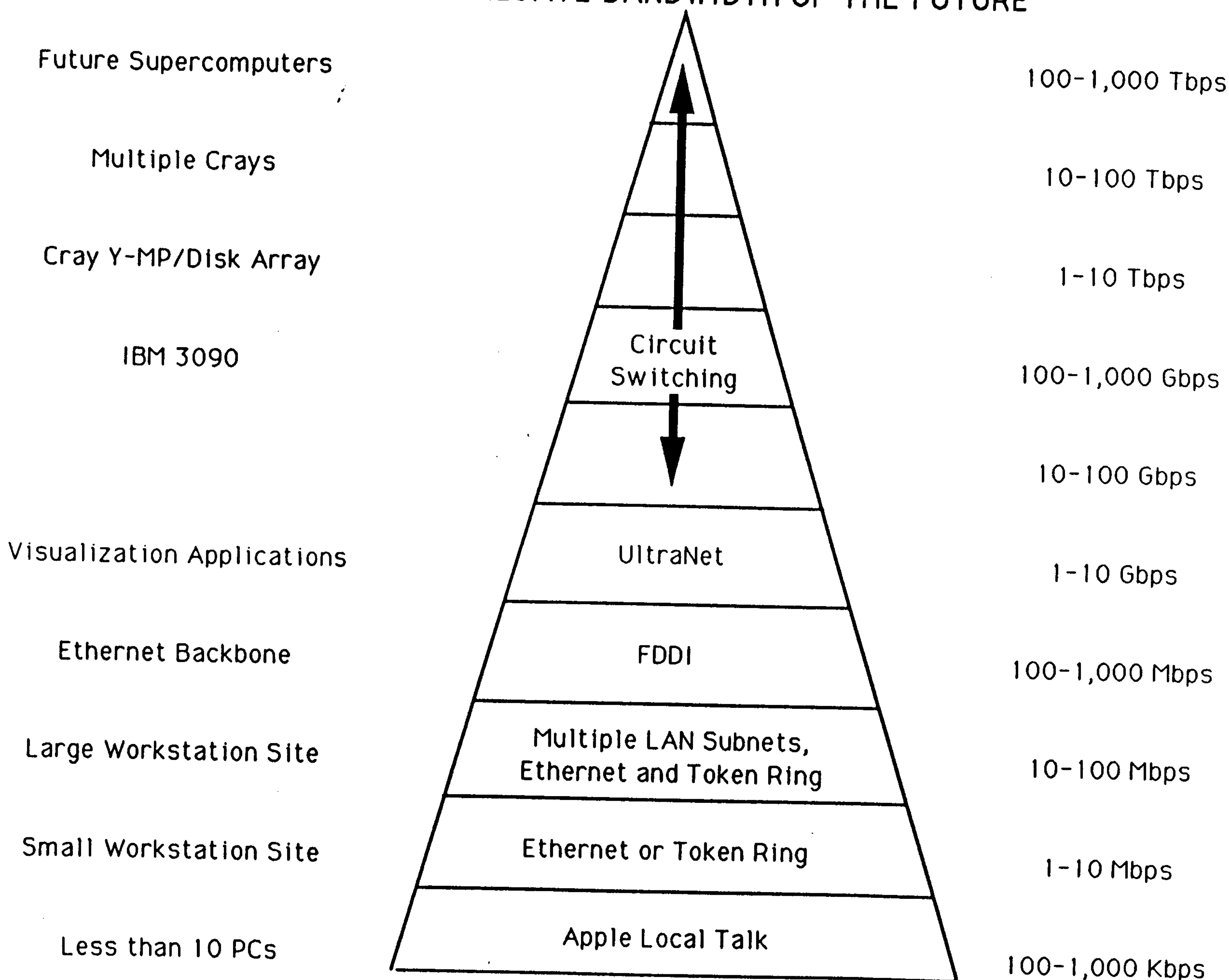
TECHNOLOGY BRIEFING

NATIONAL TEST BED NETWORK (NTBN)

TECHNOLOGY WORKING GROUP

APRIL 1991

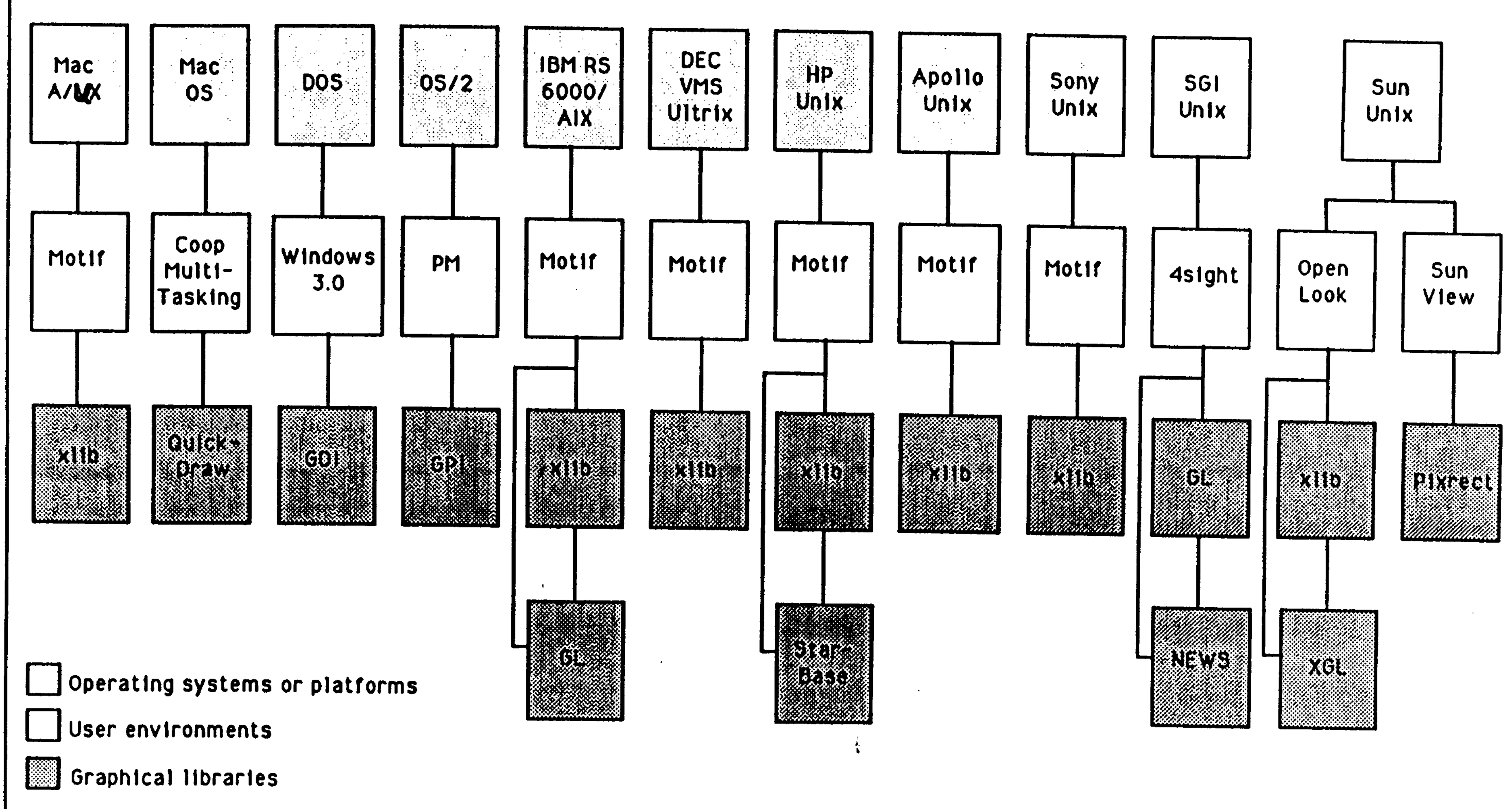
AGGREGATE BANDWIDTH OF THE FUTURE



A recent report from Electronic Trend Publications (Saratoga, Calif.) said that the need for greater capacities is driven both by the applications and the performance of the computer systems interconnected by the network. This high-capacity pyramid shows how different computer systems and applications affect the type of LANs used and the aggregate network capacity.

LAN Computing, 26 Mar 91

PLATFORMS, OPERATING SYSTEMS AND GUIs - OVERVIEW



Source: Ithaca Software

MACWEEK, 26 Feb 91

GOSIP

-ACSE-Assoc Control Service Element (ISO 8650)
-CLNP-Connectionless Network Protocol (ISO 8473)
-Connectionless Transport (ISO 8602)
-CONS-Connection Oriented Network (ISO 8348)
-Directory Services (CCITT X.500, ISO 9594)
-EDI-Electronic Data Interchange (ANSI X12)
-ES-IS-End System-Intermediate System (ISO 9542)
-FDDI-Fiber Data Distributed Interface (ISO 9314)
-FTAM-File Transfer,Access & Management (ISO 8571) & Extensions
-HDLC LAPB-Link Access Protocol, Balanced (ISO 7776)
-ODA-Office Document Architecture (ISO 8613)
-Presentation (ISO 8823)
-ROSE-Remote Operations Service Element (ISO 9072)
-RTSE-Reliable Transfer Service Element (ISO 9066)
-Session (ISO 8327)
-SNDCF-Subnetwork Dependant Convergence Facility (ISO 8473 AD1)
-Transport (ISO 8073)-Class 0 (simple), Class 4 (complex)
-VTP-Virtual Terminal Protocol (ISO 9041)
-X.25 (ISO 8208)
-IS-IS-Intermediate System-Intermediate System
-ISDN-Integrated Services Digital Network
-MHS-Message Handling System (CCITT X.400)

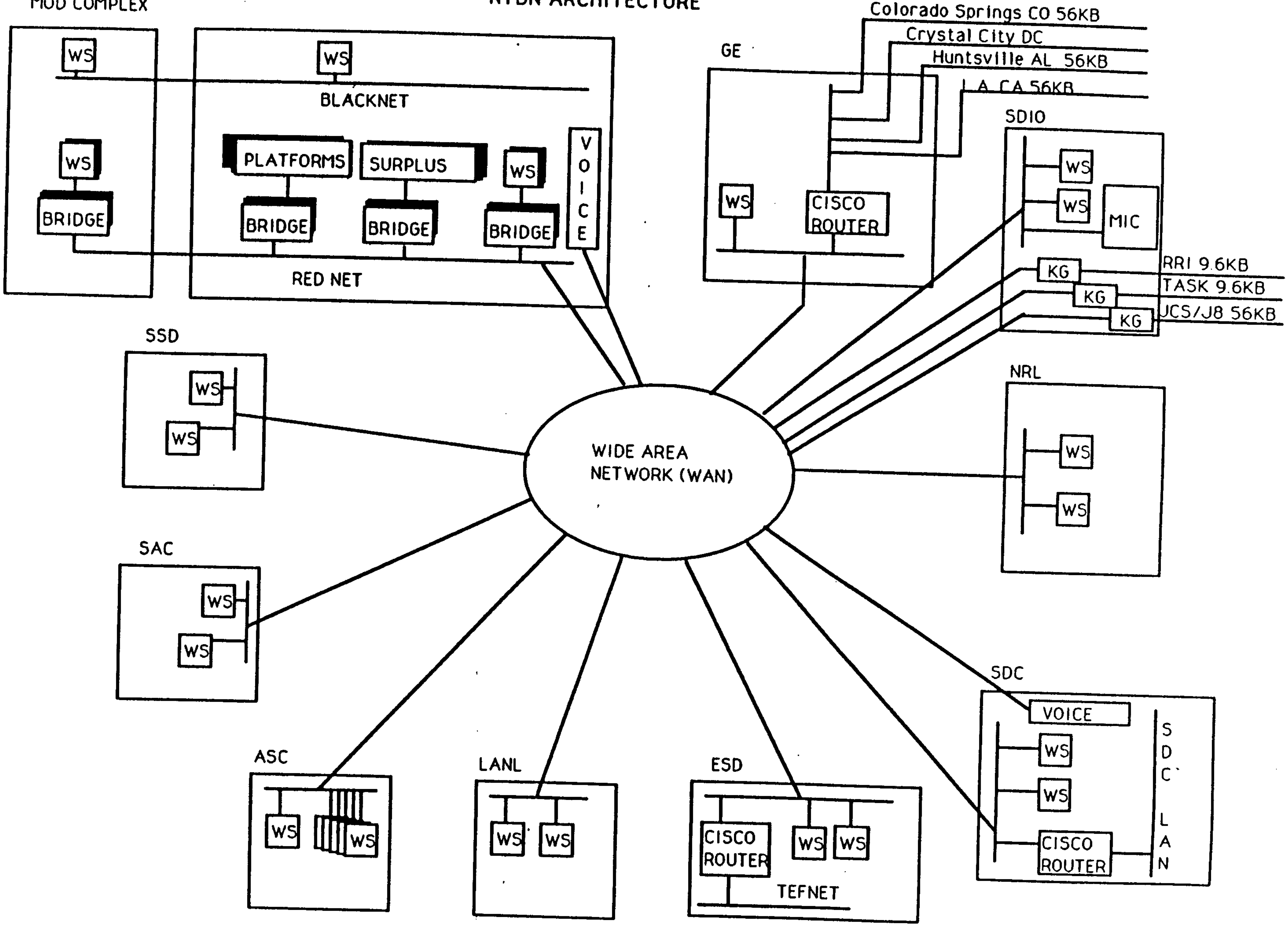
7 Appl	ISO 8649/50/50/AD1, CCITT X.217/X.227, ISO 9066, CCITT X.218/228, ISO 9072, CCITT X.219/229, ISO 9804/9805	ODA (2) ISO 8613; MHS (1) CCITT X.400 1984 (DoD SMTP); FTAM (1) EXT (2) ACSE (1) ISO 8571 (DoD FTP); VIRT TERM (2) ACSE (1) ISO 9041; EDI (3) ANSI X12; MHS (3) ROSE.RTSE (3) ACSE (1) CCITT X.400 '88; DIR SERV (3) CCITT X.500 ISO 9594 ROSE (3) ACSE (1); NET MGT (3) CMIP ROSE (3) ACSE (1) (DoD SNMP)
6 Pres	ISO 8822, ISO 8822/AD1, CCITT X.216	PRESENTATION (1) ISO 8823
5 Sess	ISO 8326, CCITT X.215, ISO 8326/AD1, ISO 8326/AD2	SESSION (1) ISO 8327
4 Tran	ISO 8072, ISO 8072/AD1, CCITT X.214	TRANSPORT-CLASS 4 (1) ISO 8073 (DoD TCP); CONNECTION-LESS TRANS (2) ISO 8602 (DoD UDP); TRANSPORT-CLASS 0 (1) ISO 8073
3 Net	ISO 8348, CCITT X.213, ISO 8348/AD1/AD2/AD3	CONNECTIONLESS TRANS PROTOCOL (CLNP) (1) ISO 8473 (DoD IP); ES-IS (2) ISO 9542; IS-IS (3); SNDCF (1) ISO 8473AD1; CONS (2) ISO 8348; CCITT X.25 PLP (1) ISO 8208; ISDN (2) CCITT Q.931
2 Data	ISO 8886, CCITT X.212	802.2,LLC TYPE1, CLASS1 (1) ISO 8802/2; HDLC LAPB (1) ISO 7776; ISDN LAPD (2) CCITT Q.921
1 Phys	CCITT X.211	802.3 (1) ISO 8802/3; 802.4 (1) ISO 8802/4; 802.5 (1) ISO 8802/5; FDDI (3) ISO 9314 ANSI X3T9.5; RS232 (1) EIA RS232-C; V.35 (1) CCITT V.35; ISDN (2) CCITT I.430 I.431

10 Base -5
10 Base -2
10 Base -T

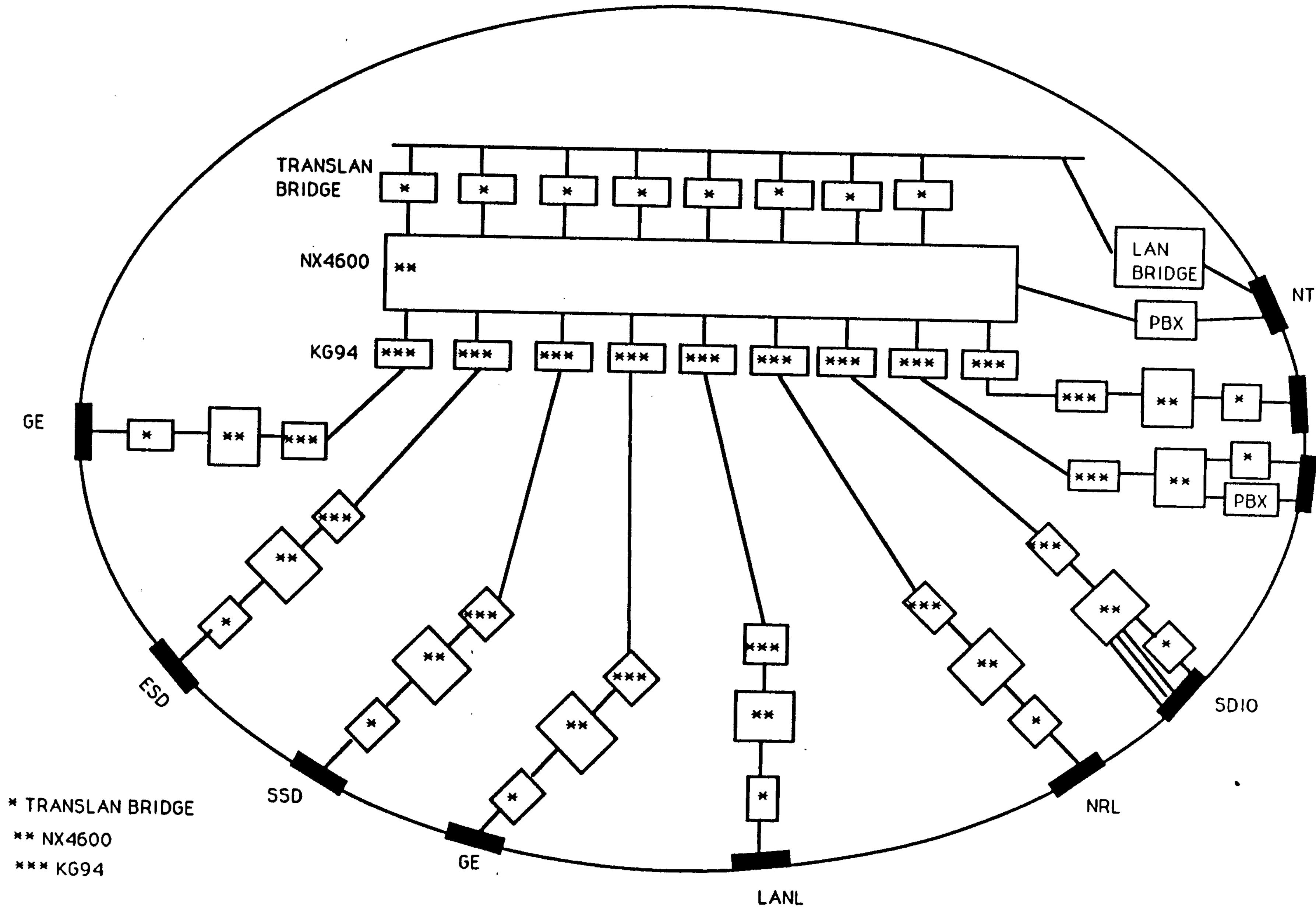
802.6 Distr Queue Dual Bus (DQDB)

(1) V1 AUG 90
(2) V2 AUG 92
(3) V3 AUG 93

NTBN ARCHITECTURE



NTBN WAN


TRANSLAN BRIDGE
NX4600
KG94
LAN BRIDGE
PBX
NTF
ASC
SDC
PBX
SDIO
NRL
LANL
GE
SSD
ESD
GE
* TRANSLAN BRIDGE
** NX4600
*** KG94

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
UNISYS/ TIMPLEX Secure FDDI	FDDI 802.3 TOKEN Ring X.25 RS-232 RS-449 V.35	IP XNS IPX	SNMP MIB BER	SAC Accredited at C2 Moving to B1 Accreditation	Meets DNSIX security -B1 Installation Base in INTEL Communities	Supports OSI Each Concetrator supports 32 single Stations Each FDDI Adapter provides 12 ports per unit for WAN interface	N/A	Serial link rate of 2.048MB/Sec per Port Supports Dual Ring FDDI backbone at 100MB/Sec per ring	Lorraine Martin 805-987-9445
VERDIX SLAN	802.3	TCP/IP	SNMP	EPL-B2 MDIA	Consistency of Labeling in Heterogeneous Enviornment	Could move to COSIP 128 NODES FDDI	UNIX VMS VLTRIX DOS A/UX XENIX	Serial link rate of 2.048MB/Sec per Port Supports Dual Ring FDDI backbone at 100MB/Sec per ring	Gary Bowles 703-378-7600
IP Router	802.3	TCP/IP	SNMP	Submit Documentation 3rd Quarter for B2	Secure IP Routing	Ready to move to COSIP 1000 NODES	N/A		

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
Boeing MLS LAN	802.3 VME DR-11 Analog/Video (Separate Cable) RS-232	TCP/IP	SNMP next year	Awaiting Technical Review Board for A1	Simultaneous Mutlilevel secure comm.	No Trunk Encription between services Plans for OSI and GOSIP No VMSOS 254 servers per network 3200 devices per network	UNIX VLTRIX	235KB/Sec end to end (TCP) 420 KB/Sec end to end UDP	Ken Takevchi 206-773-0628
LORAL Multinet Gateway MLS-100	802.3 x.25 ARPANET DDN X.25 Blacker X.25	IP Datagram	N/A	Expected on EPL during of summer of 92	IP Gateway/ Switch	Need to recode for GOSIP Not a Router	N/A	56KB/Sec 250KB/Sec	Erv Perelstein 719-594-1129

CANDIDATE PRODUCTS / AVAILABILITY

POTENTIAL PRODUCT	PHYSICAL INTERFACE STD SUPPORTED	NETWORK PROTOCOL SUPPORTED	NETWORK MGNT SUPPORT	EVALUATION STATUS	MAJOR SECURITY FEATURES	EXPANSION/ GROWTH LIMITATION	OPERATING SYSTEMS SUPPORTED	I/O CHANNEL BANDWIDTH	OTHER
GEMINI Trusted Network Processor	802.3 X.25 RS-232	Lower layers of OSI and DOD supported	NONE	Moving toward Formal Evaluation for A1	Verified Design Based on UNIX Sys 5	Interface to higher layers must be user developed Uses DES Algorithm No Network Mgnt Interface Limited X.25 Channel capability	UNIX for sys develop ment enviorn ment	1MB/Sec 802.3 19-15 KB/Sec X.25 RS-232 up to 64 channels	Mike Thompson 408-373-8500
OTHERS Motorola BLACKER & Network Encryption Unit XEROX XEU Digital DESNC Digital One Way Gateway WANG Trusted LAN I/F Unit									Jerry Hogg 602-441-2628 Vicki Beseke 602-441-3232 Frank Presson 703-442-6777 Bruce Pacot 719-260-3311 Powell Glenn 508-967-8699

STANDARDS INFORMATION

CCITT Series Recommendations

Number	Title
V.1	Equivalence between binary notation symbols and the significant conditions of a two-condition code.
V.2	Power levels for data transmission over telephone lines.
V.3	International Alphabet No. 5.
V.4	General structure of signals of International Alphabet No. 5 code for data transmission over public telephone networks.
V.5	Standardization of data signaling rates for synchronous data transmission in the general switched telephone network.
V.6	Standardization of data-signaling rates for synchronous data transmission on leased telephone -type circuits.
V.7	Definitions of terms concerning data communication over the telephone network.
V.10(X.26)	Electrical characteristics for unbalanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications.
V.11(X.27)	Electrical characteristics for balanced double-current interchange circuits for general use with integrated circuit, equipment in the field of data communications.
V.15	Use of acoustic coupling for data transmission.
V.16	Medical analogue data transmission modems.
V.19	Modems for parallel data transmission using telephone signaling frequencies.
V.20	Parallel data transmission modems standardized for universal use in the general switched telephone network.
V.21	300 bits per second duplex modem standardized for use in the general switched telephone network.
V.22	1200 bits per second duplex modem standardized for use on general switched telephone network and on leased circuits.

CCITT Series Recommendations

Number	Title
V.23	600/1200-baud modem standardized for use in the general switched telephone network.
V.24	List of definitions for interchange circuits between data terminal equipment and data circuit-terminating equipment.
V.25	Automatic calling and/or answering equipment on the general switched telephone network, including disabling of echo suppressors on manually established calls.
V.26	2400 bits per second modem standardized for use on four-wire leased circuits.
V.26bis	2400/1200 bits per second modem standardized for use in the general switched telephone network.
V.27	4800 bits per second modem with manual equalizer telephone-type circuits standardized for use on leased circuits.
V.27bis	4800/2400 bits per second modem with automatic equalizer standardized for use on leased telephone-type circuits.
V.27ter	4800/2400 bits per second modem standardized for use in the general switched telephone network.
V.28	Electrical characteristics for unbalanced double-current interchange circuits.
V.29	9600 bits per second modem standardized for use on point-to-point four-wire leased telephone type circuits.
V.31	Electrical characteristics for single-current interchange circuits controlled by contact closure.
V.35	Data transmission at 48 kilobits per second using 60-108 kHz group band circuits.
V.36	Modems for synchronous data transmission using 60-108 kHz group band circuits.

CCITT Series Recommendations

Number	Title
V.37	Synchronous data transmission at a data signaling rate higher than 72 kbits using 60-108 kHz group and circuits.
V.40	Error indication with electromechanical equipment.
V.41	Code independent error control system.
V.50	Standard limits for transmission quality of data transmission.
V.51	Organization of maintenance of international telephone type circuits used for data transmission.
V.52	Characteristics of distortion and error-rate measuring apparatus for data transmission.
V.53	Limits for the maintenance of telephone-type circuits used for data transmission.
V.54	Loop test devices for modems.
V.55	Specification for an impulse noise measuring instrument for telephone-type circuits.
V.56	Comparative tests for modems for use over telephone-type circuits.
V.57	Comprehensive data test set for high data signaling rates.
X.1	International user classes of service in public data networks.
X.2	International user services and facilities in public data networks.
X.3	Packet assembly/disassembly facility (PAD) in a public data network.
X.4	General structure of signals of International Alphabet No. 5 code for data transmission over public data networks.
X.15	Definitions of terms concerning public data networks.
X.20	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for start-stop transmission services on public data networks.
X.20bis	Use on public data networks of data terminal equipment (DTE) which is designed for interfacing to asynchronous duplex V-series modems.

CCITT Series Recommendations

Number	Title
X.21	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for synchronous operation of public data networks.
X.21bis	Use on public data networks of data terminal equipments which is designed for interfacing to synchronous V-series modems.
X.22	Multiplex DTE/DCE interface for user classes 3-6.
X.24	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) on public data networks.
X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet made on public data networks.
X.26(V.10)	Electrical characteristics for unbalanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications.
X.27(V.11)	Electrical characteristics for balanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications.
X.28	DTE/DCE Interface for a start-stop mode data terminal equipment accessing the packet assembly/disassembly facility (PAD) in a public data network situated in the same country.
X.29	Procedures for the exchange of control information and user data between a packet assembly/disassembly facility (PAD) and a packet mode DTE or another PAD.
X.40	Standardization of frequency-shift and modulated transmission systems for the provision of telegraph and data channels by frequency division of a group.
X.50	Fundamental parameters of a multiplexing scheme for the international interface between synchronous data networks.
X.50bis	Fundamental parameters of a 48 kbit/s user data signaling rate transmission scheme for the international interface between synchronous data networks.

CCITT Series Recommendations

Number	Title
X.51	Fundamental parameters of a multiplexing scheme for the international interface between synchronous data networks.
X.51bis	Fundamental parameters of a 48 kbit/s user data signaling rate transmission scheme for the international interface between synchronous data networks using 10-bit envelope structure.
X.52	Method of encoding anisochronous signals into a synchronous bearer.
X.53	Numbering of channels on international multiplex links at 64 kbit/s.
X.54	Allocation of channels on international multiplex links at 64 kbit./s.
X.60	Common channel signaling for circuit switched data applications.
X.61	Signaling system No. 7- Data user part.
X.71	Decentralized terminal and transit control signaling system on international circuits between synchronous dat networks.
X.75	Terminal and transit call control procedures and data transfer system on international circuits between packet-switched data networks.
X.80	Interworking of interexchange signaling systems for circuit switched data services.
X.87	Principles and procedures for realization of international user facilities and network utilities in public data networks.
X.92	Hypothetical reference connections for public synchronous data networks.
X.96	Call progress signals in public data networks.
X.110	Routing principles for international public data services through switched public data networks of the same type.
X.121	International numbering plan for public data networks.
X.130	Provisional objectives for call set-up and clear-down times in public synchronous data networks (circuit switching).
X.132	Provisional objectives for grade of service in international data communications over circuit switched public data networks.

CCITT Series Recommendations

Number	Title
X.150	DTE and DCE test loops in public data networks.
X.180	Administrative arrangements for international closed user groups (CUGs).

International Organization for Standardization

Number	Title
ISO 646	Seven-bit character set for information processing interchange- 1973, confirmed 1979.
ISO 1155	Information processing - Use of longitudinal parity to detect errors in information messages - 1978.
ISO 1177	Information processing - Character structure for start/stop and synchronous transmission - 1973, revision being balloted.
ISO 1745	Information processing - Basic mode control procedures for data communications systems - 1975, revision being balloted.
ISO 2022	Code extension techniques for use with ISO seven-bit coded character set - 1973.
ISO 2110	Data communications - 25 pin DTE/DCE interface connector and pin assignments - 1980.
ISO 2111	Data communication - Basic mode control procedures - Code independent information transfer - 1972, revision being balloted.
ISO 2593	Connector pin allocations for use with high speed data terminal equipment - 1973, revision being balloted.
ISO 2628	Basic mode control procedures - Complements - 1973, confirmed 1979.
ISO 3309	Data communication - High level data link control procedures- frame structure - 1979, revision being balloted.
ISO 4335	Data communication - High level data link control procedures - Elements of procedures 1979 - Addendum 1, 1979; Addendum II, 1981.
ISO 4902	Data communication - 37-pin DTE/DCE interface connector and pin assignments - 1980.
ISO 4903	Data communication - 15-pin DTE/DCE interface connector and pin assignments - 1980.
ISO 6159	Data communication - HDLC unbalanced classes of procedures - 1980.
ISO 6256	Data Communication - HDLC balanced class of procedures - 1980.

American National Standards Institute

Number	Title
X3.1-1976	Synchronous signaling rates for data transmission.
X3.4-1977	Code for information interchange.
X3.15-1976	Bit sequencing of the American National Standard Code for information interchange in serial-by-bit data transmission.
X3.16-1976	Character structure and character parity sense for serial-by-bit data communication in the American National Standard Code for information interchange.
X3.24	Signal quality at interface between data terminal equipment and synchronous data communication equipment for serial data transmission (adopts EIA RS-334-A) - pending resolution of negative ballot.
X3.25 - 1976	Character structure and character parity sense for parallel by-bit communication in the American National Standard Code for Information Interchange.
X3.28-1976	Procedures for the use of communication control characters of American National Standard Code for Information Interchange in specified data communication links.
X3.36-1975	Synchronous high-speed data signaling rates between data terminal equipment and data communication equipment.
X3.41-1974	Code extension techniques for use with 7 bit coded character set of American National Standard Code for Information Interchange.
X3.44-1974	Determination of the performance of data communication systems.
X3.57-1977	Structure of formatting message headings for information interchange using the American National Standard Code for information interchange for data communication system control.
X3.66-1979	For advanced data communications control procedures (ADCCP).
X3.79-1981	Determination of performance of data communication systems that use bit-oriented procedures.
X3.92-1981	Data encryption algorithm.

Several other organizations are quite active in the standards area. The European Computer Manufacturers Association (ECMA) has published some valuable documents on HDLC and local area networks (ECMA, 114 Rue du Rhone, CH-1204 Geneva, Switzerland). The Electronics Industries Association has many published standards and provides a catalog of these documents (ELA, 2001 Eye St., N.W., Washington, D.C. 20006). The National Communications System (NCS), (General Services Administration, Specification Distribution Board, Building 197, Washington Navy Yard, Washington, D. C. 20407) and the National Bureau of Standards (write to the NTIS) publish standards for government organizations.

NTT's STANDARDS

Standard	Source
I. APPLICATION PROGRAMMING INTERFACE	
Programming Languages:	
Cobol	ISO/SAA
Fortran	ISO/SAA
C	ANSI/SAA
Database access language:	
SQL	ISO/JIS/SAA
Interface language:	
Structured Transaction Definition Language (STDL)	DEC's
Coded Character sets	ISO
Coded kanji character sets	JIS
II. SYSTEM INTERCONNECTION INTERFACE	
1. LAN topology support:	
Ethernet	IEEE
Token Ring	IEEE
2. Wide area network:	
X.25	ISO
Telnet	Internet
RPC	OSF
3. LAN protocol support:	
TCP/IP	Internet
X.400	ISO
FTAM	ISO
SMTP	ISO
SNMP	Internet
OSI Network Management	ISO
FTP	Internet
OSI TP	ISO
UDP	Internet
III. HUMAN USER INTERFACE	
OSF/Motif	OSF
Open Look	UI
Presentation Manager	Microsoft
CUA	IBM
FIM	ISO

Elements of these networking standards are at the core of NTT's MIA.

V - SERIES STANDARDS

X.20 bis	Asynchronous for V series
X.21 bis	Synchronous for V series
V.21	300 bps switched lines
V.22	1200 bps leased lines
V.22 bis	2400 bps switched lines
V.23	300/1200 bps switched lines
V.26	2400 bps leased lines
V.26 bis	2400/1200 bps switched lines
V.26 ter	2400 bps switched or leased lines
V.27	4800 bps manual equalizer, leased lines
V.27 bis	4800/2400 bps automatic, equalizer leased lines
V.27 ter	4800/2400 bps switched lines
V.29	9600 bps leased lines
V.32	9600 bps switched lines
V.35	48 kbits/s using 60- 108-kHz bands
V.25	Automatic call unit

CCITT and Bell/AT&T Modem Types

Modem Type	CCITT Standard	Transmission Mode	Circuit Type	Sync/ Async	Type of Modulation	Speed (bit/s)
103J/113D	V.21	FDX	2-W/Dial	Async	FSK	300
202S	V.23	HDX	2-W/Dial	Async	FSK	1200
202T	V.23	FDX	4-W/Leased	Async	FSK	1200
212A	V.22	FDX	2-W/Dial	Async or Sync	FSK	300
				or Sync	2PSK	1200
201C	V.26bis	FDX	2-W/4-W Dial/Leased	Sync	4PSK	2400
201B	V.26	FDX	4-W/Leased	Sync	4PSK	2400
208A	V.27bis	FDX	4-W/Leased	Sync	8PSK	4800
208B	V.27ter	FDX	2-W/Dial	Sync	8PSK	4800
209	V.29	FDX	4-W/Leased	Sync	16QAM	9600

EIA and RELATED STANDARDS

SERIES	DESCRIPTION	RELATED STANDARDS
RS232-C	Interface between data terminal equipment and data communication equipment employing serial binary data interchange	CCITT V.24, V.28; ISO 2110
RS269-B	Synchronous signaling rates for data transmission	CCITT V.5, V.6, X.1; ANSI X3.1; FED-STD 1013; FIPS 22-1
RS334-A	Signal quality at interface between data terminal equipment and synchronous data communication equipment for serial data transmission	ANSI X3.24
RS363	Standard for specifying signal quality for transmitting and receiving data-processing terminal equipments using serial data transmission at the interface with non-synchronous data communication equipment	None
RS366-A	Interface between data terminal equipment and automatic calling equipment for data communication	CCITT V.25
RS404	Standard for start-stop signal quality between data terminal equipment and nonsynchronous data communication equipment	None
RS410	Standard for the electrical characteristics of class A closure interchange circuits	None
RS422-A	Electrical characteristics of balanced voltage digital interface circuits	CCITT V.11, X.27; FED-STD 1020A
RS423-A	Electrical characteristics of unbalanced voltage digital interface circuits	CCITT V.10, X.26; FED-STD 1030A
RS449	General-purpose 37- and 9-position interface for data terminal equipment and data circuit-terminating equipment employing serial binary data interchange	CCITT V.24, V.54, X.21bis

APPENDIX F

GENERIC ARCHITECTURE DIAGRAMS

NTB NETWORK Security Architecture

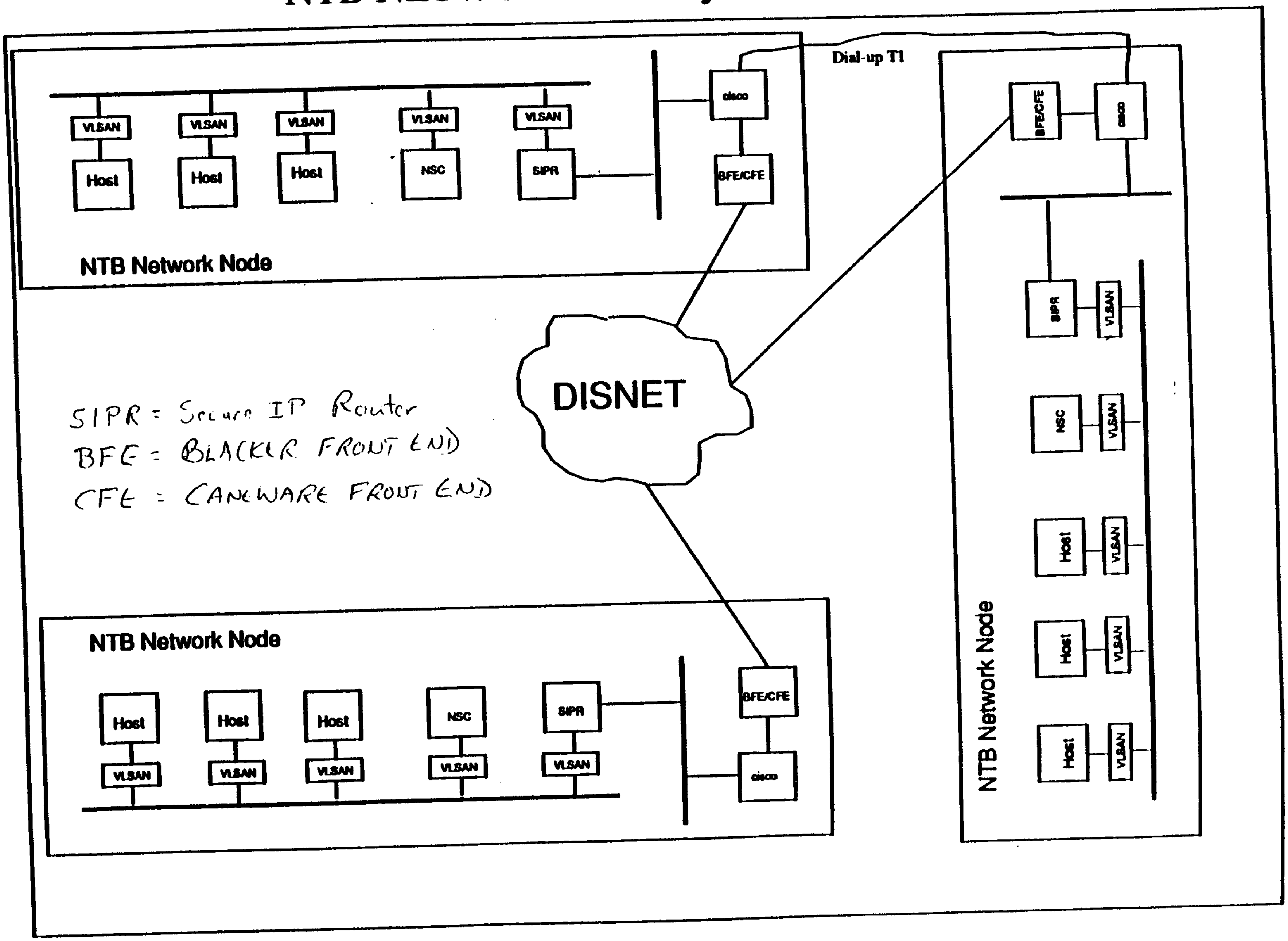
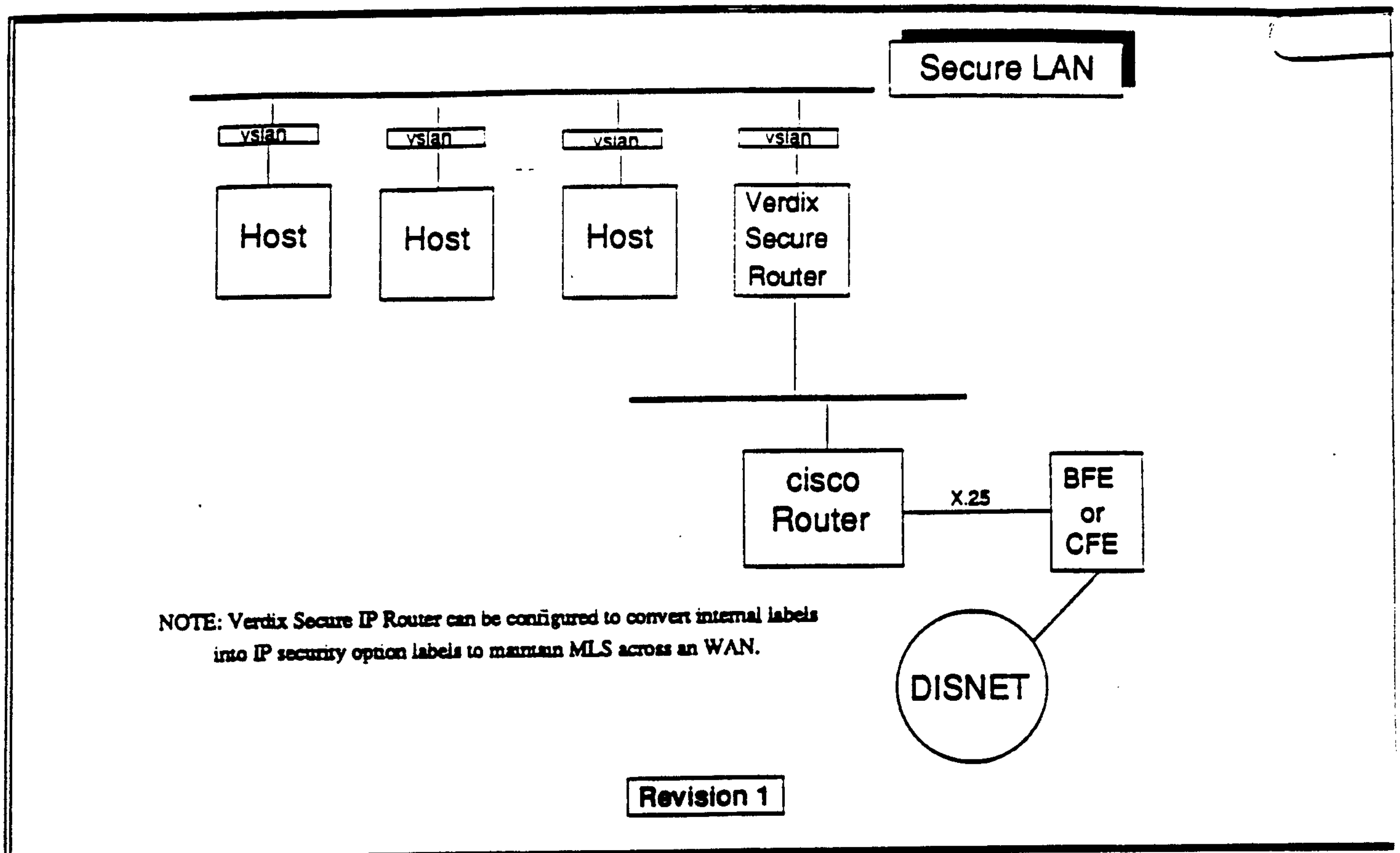


Figure E-1. NTBN Architecture Using VSLAN, DISNET and CFE/BFE (Source: H. Weiss paper)



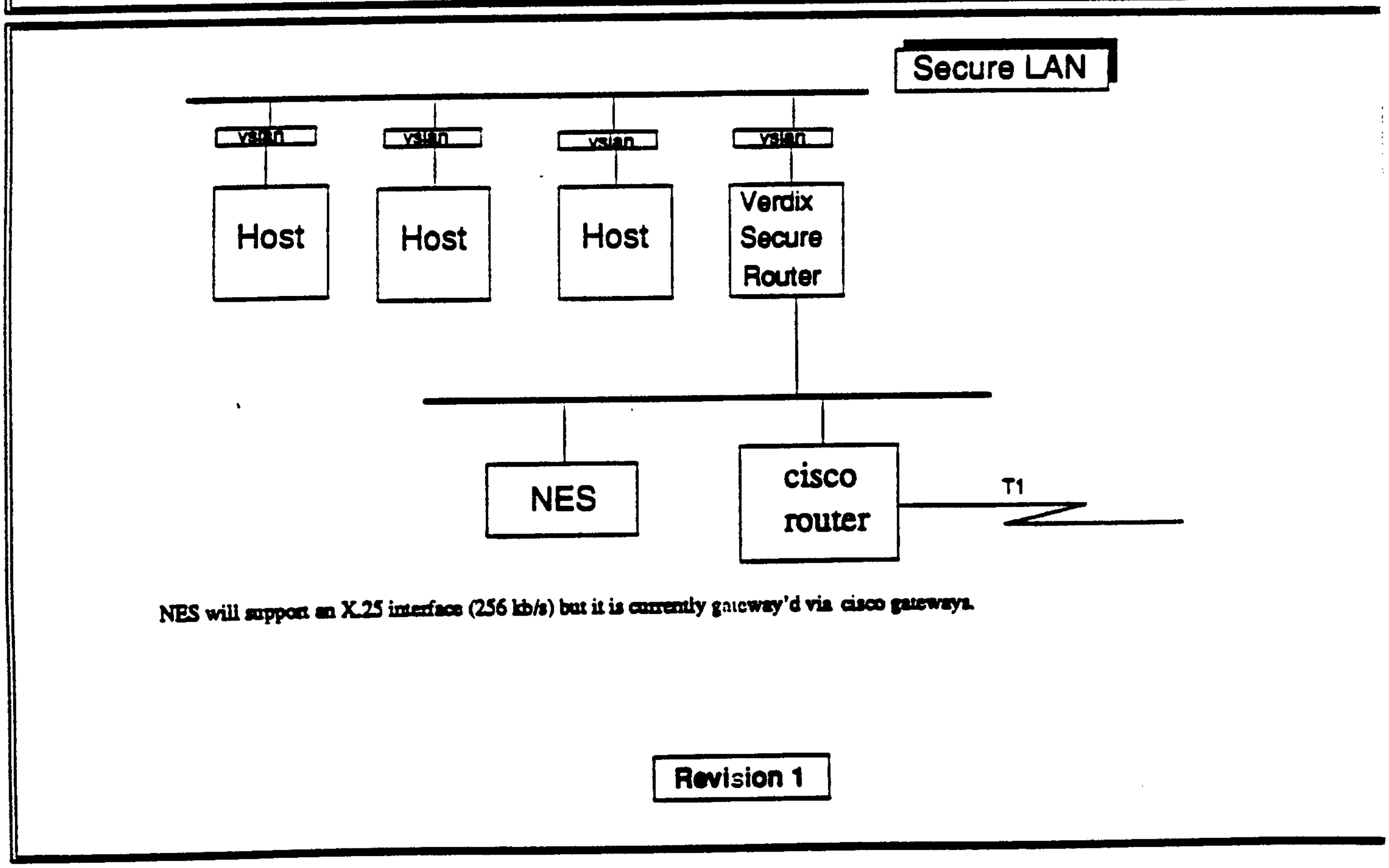
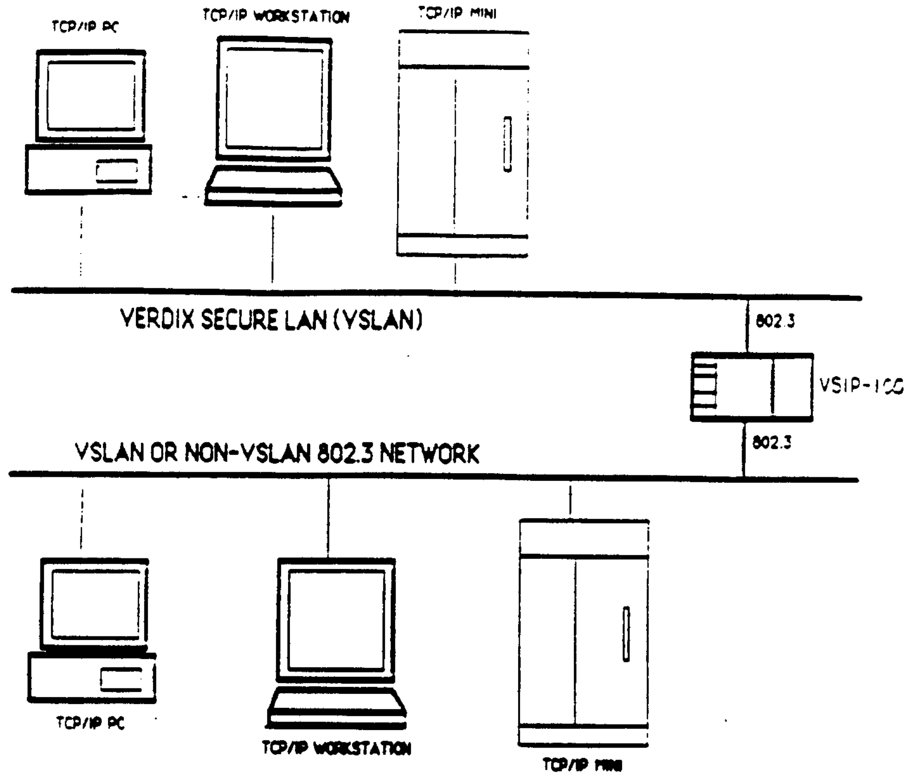


Figure E-2. Applications for Verdix Secure IP Router (Source: H. Weiss paper)



Verdix Secure Local Area Network (VSLAN®)

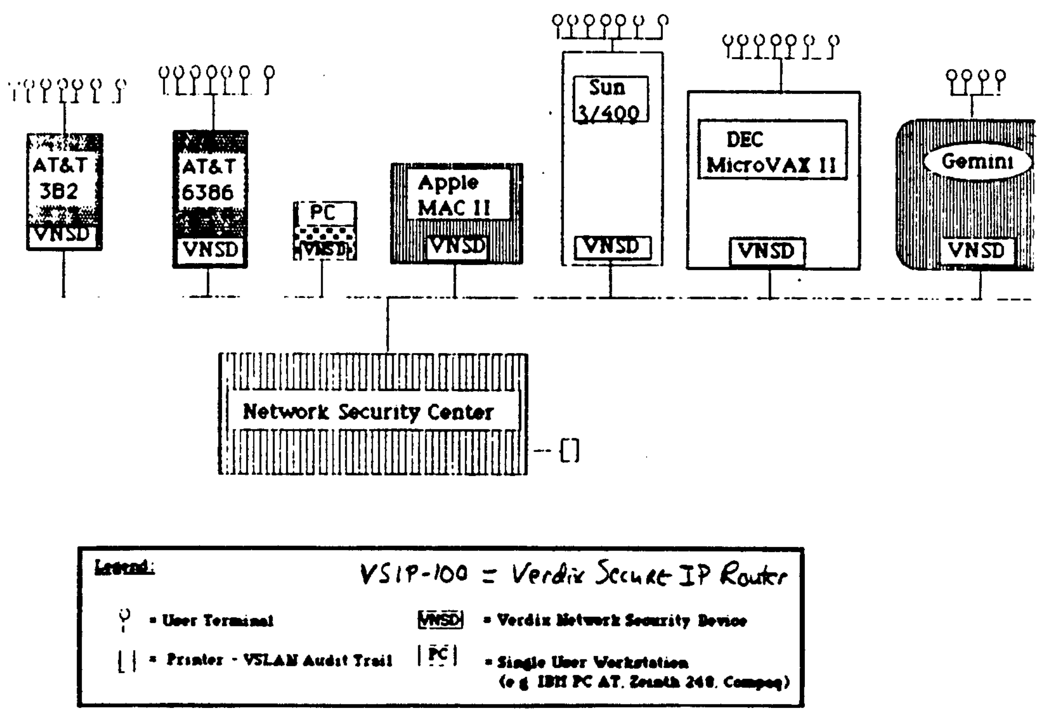
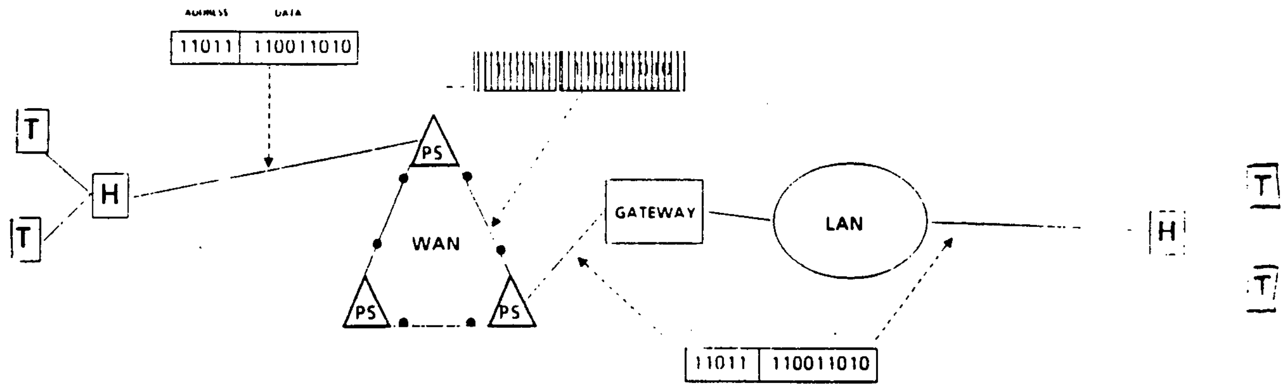
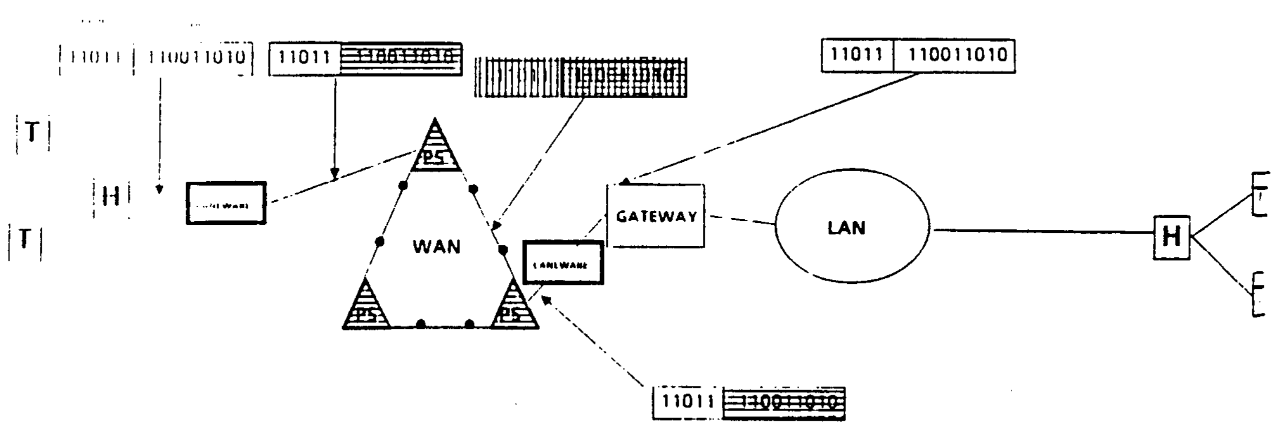


Figure E-3. Verdix VSLAN Diagrams (Source: Verdix literature)

NETWORK ENVIRONMENT W/O CANEWARE



NETWORK ENVIRONMENT WITH CANEWARE



NETWORK ENVIRONMENT WITH CANEWARE AND NES

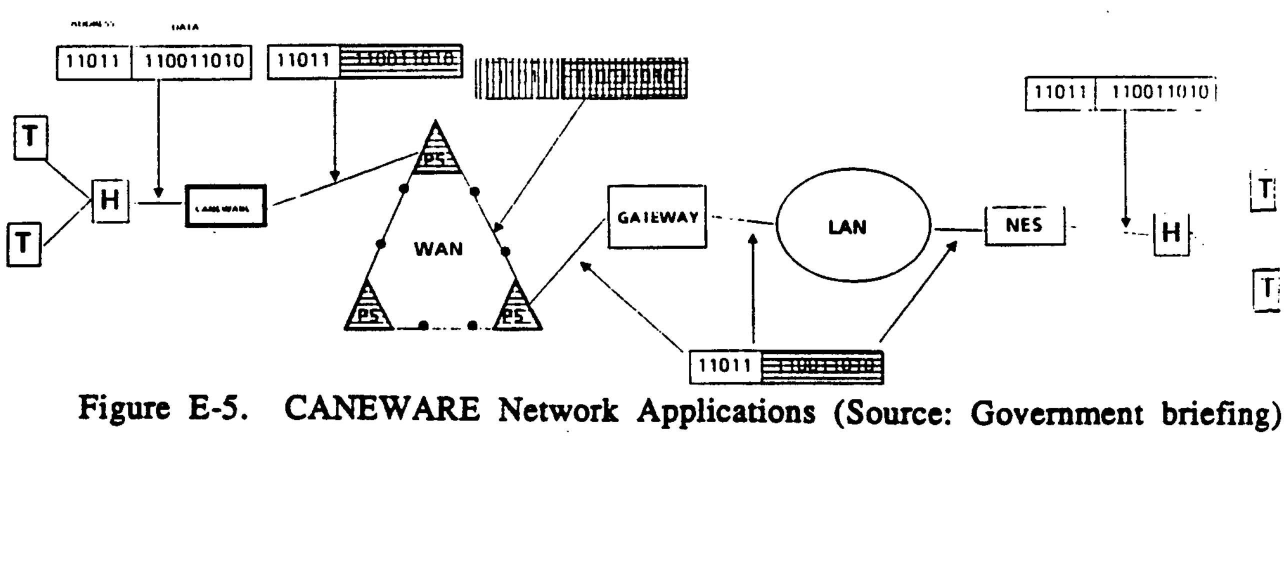


Figure E-5. CANEWARE Network Applications (Source: Government briefing)

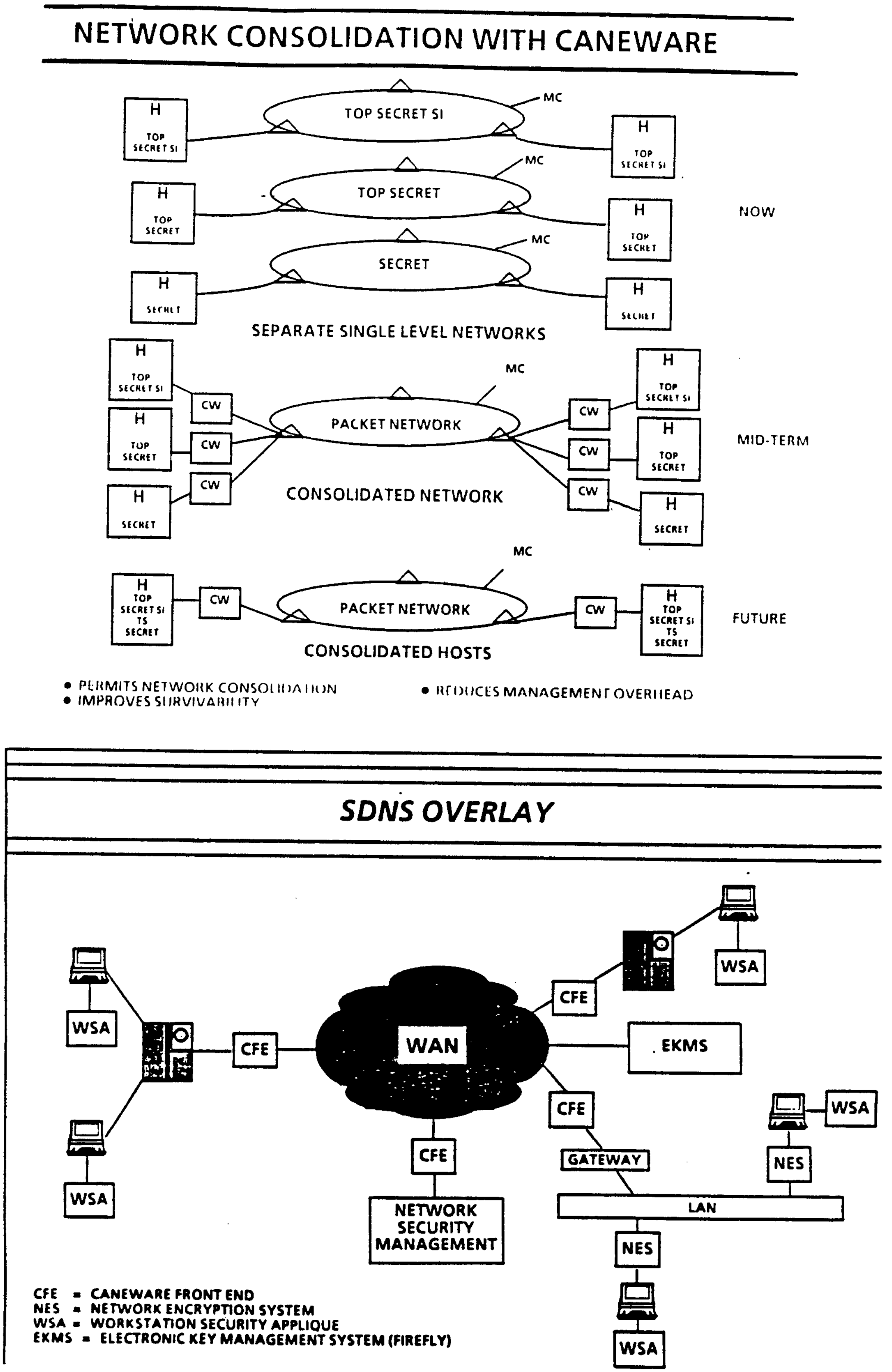
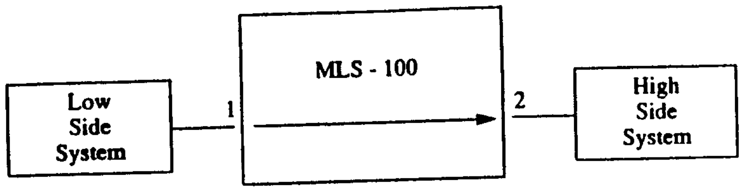
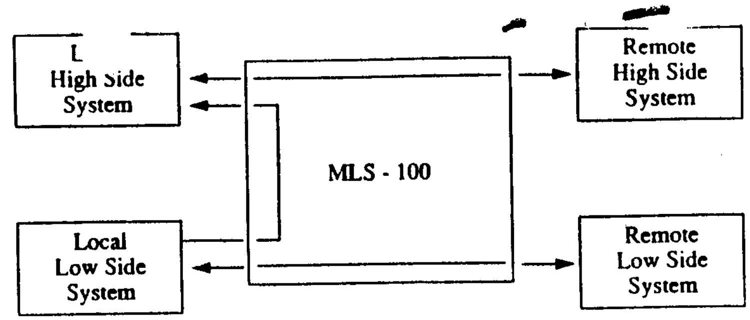


Figure E-6. CANEWARE and NES Network Applications (Source: Government briefing)



Low - to - High

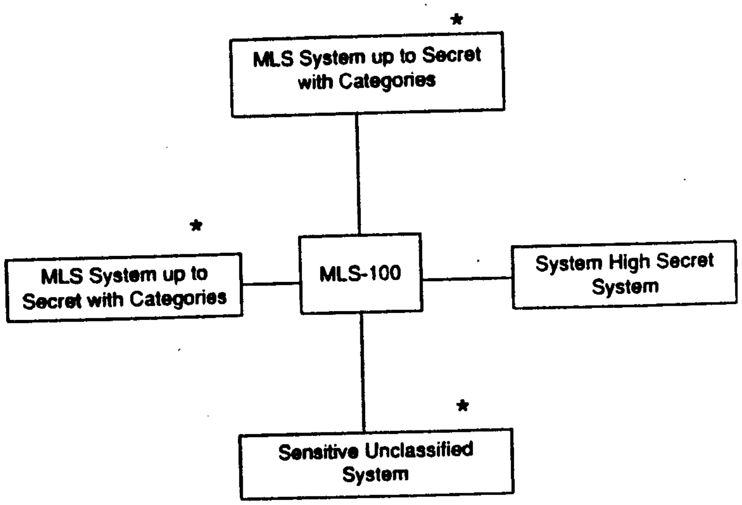
Figure 2-5. MLS-100 One-Way Flow Enforcement



Prohibited:

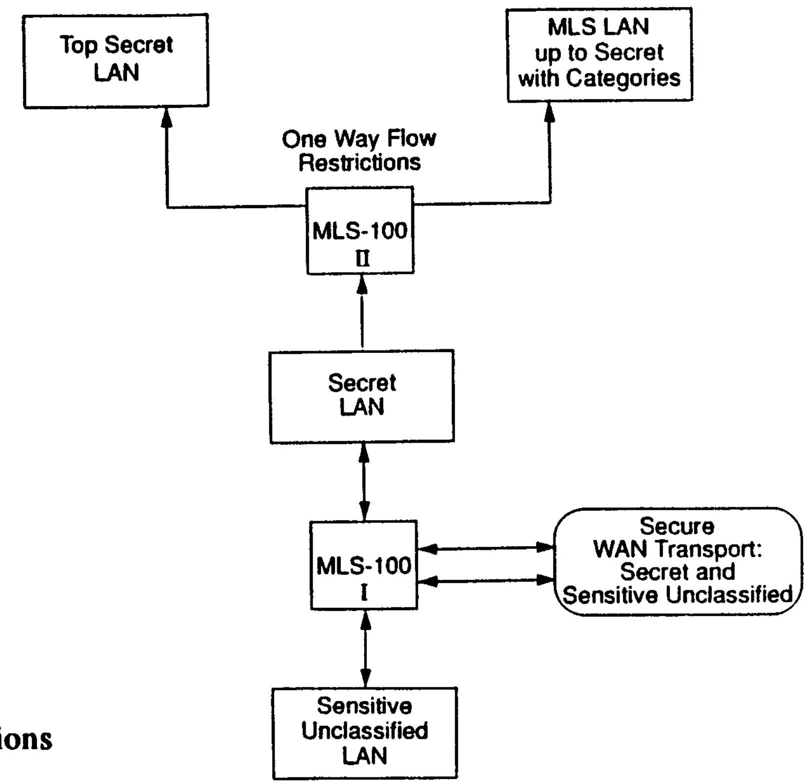
Local High to Local Low
Local High to Remote Low
Local Low to Remote High
Remote Low to Local High

Flow Restrictions, Interconnected System High Example



* - Minimum User Clearance of Secret

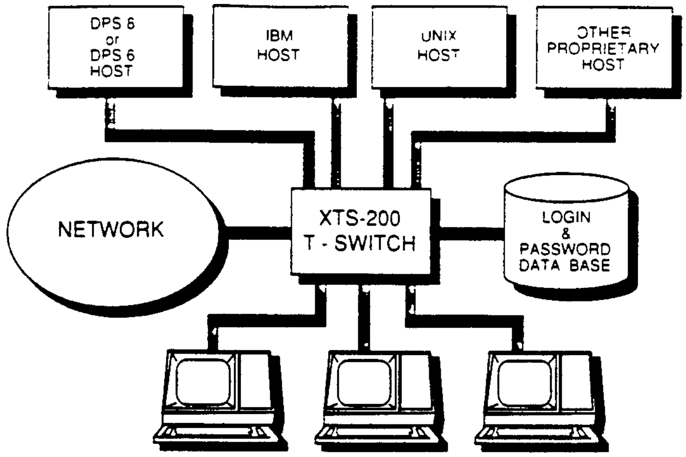
Interconnection Involving MLS Systems



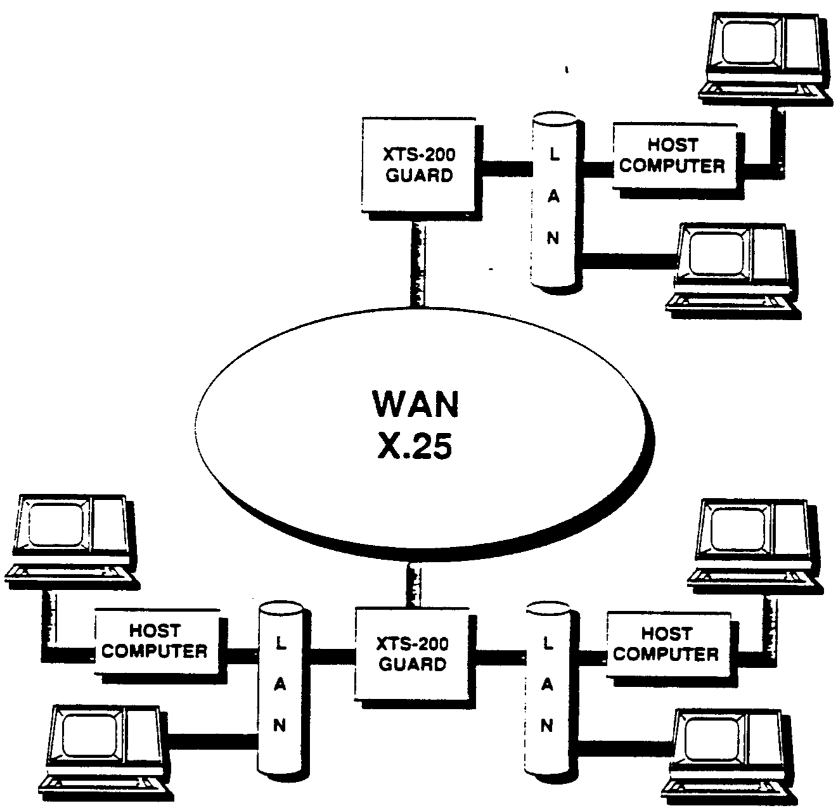
On-Site Connections to External Systems

Figure E-7. Loral MLS-100 Network Applications

(Source: Loral literature)

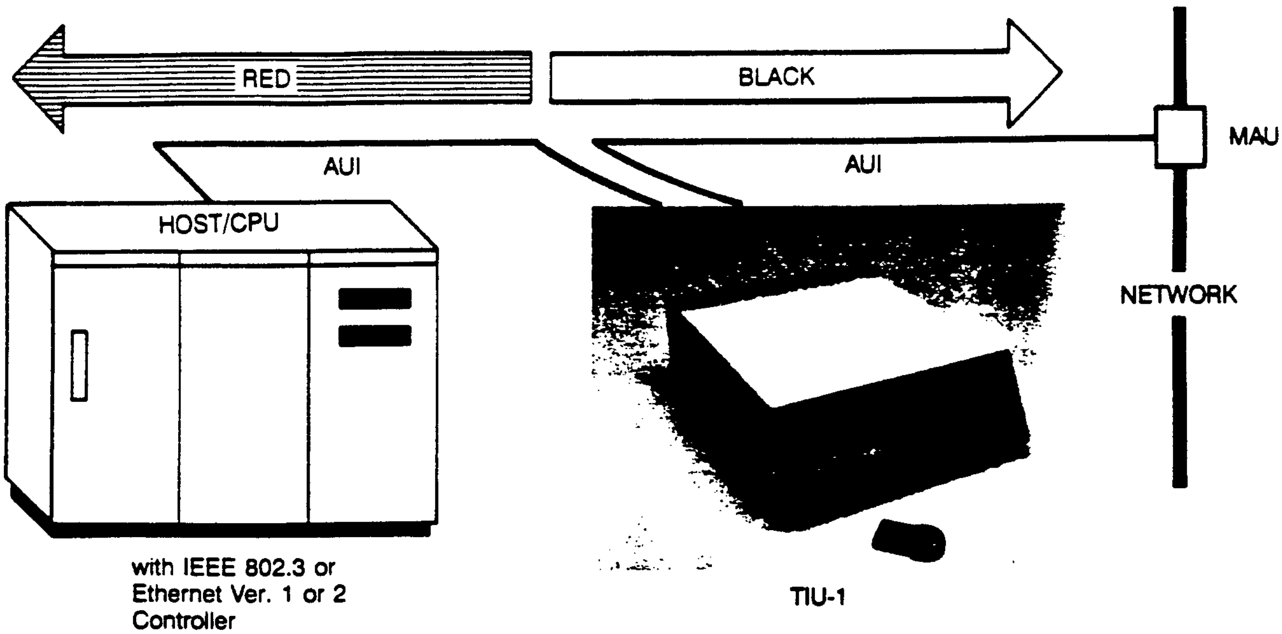


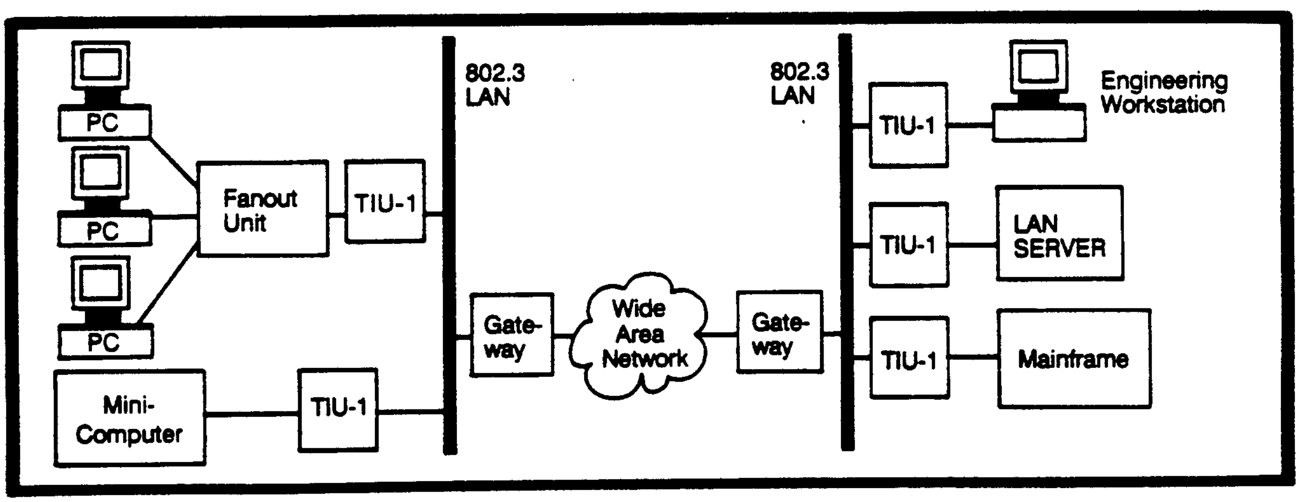
TRUSTED SWITCH



NETWORK GUARD

Figure E-8. HFSI XTS-200 Network Applications (Source: HFSI literature)





TIU-1 Provides End-to-End Encryption Over Both Local Area and Wide Area Networks

Figure E-9. Wang TIU Network Applications (Source: Wang literature)
(Note: Xerox XEU applications are similar)